



University
of Glasgow

He, Ying (2014) *Generic security templates for information system security arguments: mapping security arguments within healthcare systems*. PhD thesis.

<http://theses.gla.ac.uk/5773/>

Copyright and moral rights for this thesis are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Generic Security Templates for information system security arguments

Mapping security arguments within healthcare systems

Ying He



Doctor of Philosophy
School of Computing Science
University of Glasgow
2014

Abstract

Industry reports indicate that the number of security incidents happened in healthcare organisation is increasing. Lessons learned (i.e. the causes of a security incident and the recommendations intended to avoid any recurrence) from those security incidents should ideally inform information security management systems (ISMS). The sharing of the lessons learned is an essential activity in the “follow-up” phase of security incident response lifecycle, which has long been addressed but not given enough attention in academic and industry.

This dissertation proposes a novel approach, the Generic Security Template (GST), aiming to feed back the lessons learned from real world security incidents to the ISMS. It adapts graphical Goal Structuring Notations (GSN), to present the lessons learned in a structured manner through mapping them to the security requirements of the ISMS. The suitability of the GST has been confirmed by demonstrating that instances of the GST can be produced from real world security incidents of different countries based on in-depth analysis of case studies.

The usability of the GST has been evaluated using a series of empirical studies. The GST is empirically evaluated in terms of its given effectiveness in assisting the communication of the lessons learned from security incidents as compared to the traditional text based approach alone. The results show that the GST can help to improve the accuracy and reduce the mental efforts in assisting the identification of the lessons learned from security incidents and the results are statistically significant. The GST is further evaluated to determine whether users can apply the GST to structure insights derived from a specific security incident. The results show that students with a computer science background can create an instance of the GST.

The acceptability of the GST is assessed in a healthcare organisation. Strengths and weaknesses are identified and the GST has been adjusted to fit into organisational needs. The GST is then further tested to examine its capability to feed back the security lessons to the ISMS. The results show that, by using the GST, lessons identified from security incidents from one healthcare organisation in a specific country can be transferred to another and can indeed inform the improvements of the ISMS.

In summary, the GST provides a unified way to feed back the lessons learned to the ISMS. It fosters an environment where different stakeholders can speak the same language while exchanging the lessons learned from the security incidents around the world.

Acknowledgements

Many thanks to my parents for the numerous support; and of course to Prof. Christopher Johnson and Dr. Karen Renaud, my faithful PhD supervisors.

Declaration

Some of the material presented within this dissertation has previously been published in the following papers:

- Y. He, C.W. Johnson, M. Evangelopoulou and Z.S. Lin. Diagraming approach to structure the security lessons: Evaluation using Cognitive Dimensions. The 7th International Conference on Trust & Trustworthy Computing, 2014, Crete, Greece.
- Y. He, C.W. Johnson, Y. Lu, and A. Ahmad. Improving the exchange of lessons learned in security incident reports: Case studies in the privacy of electronic patient records. The 8th IFIP WG 11.11 International Conference on Trust Management, 2014, Singapore.
- Y. He, C.W. Johnson, Y. Lu and Y. Lin. Improving the Information Security Management: An Industrial Study in the Privacy of Electronic Patient Records. IEEE CBMS 2014 The 27th International Symposium on Computer-Based Medical Systems, 2014, New York, US.
- Y. He, C.W. Johnson, K. Renaud and Y. Lu and S. Jebriel. An empirical study on the use of the Generic Security Template for structuring the lessons from information security incidents. The 6th International Conference of Computer Science and Information Technology, 2014, Amman, Jordan.
- Y. He, and C.W. Johnson. Generic security cases for information system security in healthcare systems. The 7th IET International Conference on System Safety, Incorporating the Cyber Security Conference 2012, Edinburgh, UK.

Some recent papers related to this dissertation have been submitted and are now under review:

- Y. He, and C.W. Johnson. Improving the Information Security Management in Healthcare: An Industrial Study in the Protection of Electronic Patient Records. Submitted.
- Y. He, and C.W. Johnson. Generic Security Templates for structuring the exchange of lessons from information security incidents in healthcare organisations. Submitted.

I declare that this dissertation was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

(Ying He)

To my family.

Table of Contents

1	Introduction	1
1.1	Background	1
1.1.1	Information security incident	1
1.1.2	Legislative and government initiatives	2
1.1.3	Information Security Management Systems (ISMS)	3
1.1.4	Security incident response	3
1.1.5	Current methods in sharing the lessons learned	4
1.2	Dissertation statement	5
1.2.1	Hypothesis	5
1.2.2	Definitions	7
1.2.3	Research questions	8
1.3	Dissertation structure	8
2	Review of Literature	11
2.1	Information security	12
2.1.1	Definition of information security	12
2.1.2	Security threats, vulnerabilities, and countermeasures	12
2.1.3	Information security in healthcare systems	13
2.2	Information Security Management Systems (ISMS)	15
2.2.1	Information Security Management Systems	15
2.2.2	Information Security Management Systems framework	15
2.2.3	Security standards and guidelines	16
2.2.4	Strengths and weaknesses of security standards/guidelines	18
2.2.5	Security requirement modelling	19
2.2.6	ISMS and incident learning	19
2.3	Security incident management	20
2.3.1	Security incident	20

2.3.2	Security incident response lifecycle	20
2.4	Incident learning	22
2.4.1	Post-incident activities	22
2.4.2	Imbalanced focus in security incident learning	23
2.4.3	Current initiatives in incident learning	23
2.5	Sharing of the lessons learned	24
2.5.1	Lessons learned sharing through agent organisations	24
2.5.2	Lessons learned sharing through incident dissemination	25
2.5.3	Lessons learned sharing in healthcare organisations	27
2.6	Context of the research	28
3	The Generic Security Template	31
3.1	Assurance cases	31
3.1.1	Arguments and assurance cases	31
3.1.2	Graphical notations	33
3.2	Goal structuring notations (GSN)	35
3.2.1	GSN elements and notations	35
3.2.2	Goal decomposition methods	36
3.2.3	Safety arguments and the GSN	37
3.2.4	Security arguments and the GSN	38
3.3	The Generic Security Template	38
3.3.1	Definition of the Generic Security Template	40
3.3.2	The Generic Security Template and assurance cases	41
3.3.3	Creation of instances of the Generic Security Template	41
3.3.4	Pre-requisites to apply the Generic Security Template	46
3.4	The Generic Security Template Pattern	46
3.4.1	GSN Pattern	46
3.4.2	The Generic Security Template Pattern	47
3.5	Evaluation of the Generic Security Template	49
3.6	Summary	50
4	Instances of the Generic Security Template	51
4.1	Veterans Affairs (VA) data leakage incident 2006	51
4.1.1	Case description	51
4.1.2	Instance of the Generic Security Template	52
4.2	Veterans Affairs (VA) data leakage incident 2007	54

4.2.1	Case description	54
4.2.2	Instance of the Generic Security Template	56
4.3	Shenzhen data leakage incident 2008	58
4.3.1	Case description	58
4.3.2	Instance of the Generic Security Template	60
4.4	NHS Surrey IT Asset Disposal Incident 2013	61
4.4.1	Case description	61
4.4.2	Instance of the Generic Security Template	63
4.5	Discussion	66
4.5.1	Case selection	66
4.5.2	Success criteria	66
4.5.3	Time and efforts	67
4.6	Summary	68
5	Comparison of the Generic Security Template with traditional Text-based Approach - An Empirical Evaluation	69
5.1	Related work	70
5.1.1	Graphical notation evaluation	70
5.2	Experiment design	70
5.2.1	Experiment design and scope	70
5.2.2	Ethical approval	72
5.2.3	Experiment variables	72
5.2.4	Experiment material	74
5.2.5	Pilot study	75
5.2.6	Experiment task design	76
5.3	Experiment procedures	77
5.3.1	Experiment treatment	77
5.3.2	Participants	78
5.3.3	Training of the participants	78
5.3.4	Experiment execution	78
5.3.5	Analysing the data	79
5.4	Results	80
5.4.1	Results for accuracy (lessons learned)	80
5.4.2	Results for accuracy (security arguments)	83
5.4.3	Results for efficiency (time)	85

5.4.4	Results for task load index (TLX)	86
5.5	Subjective feedback	86
5.5.1	Evaluation using Cognitive Dimensions	87
5.5.2	Overall experience	89
5.6	External and internal threats	92
5.6.1	Internal validity	92
5.6.2	External validity	93
5.7	Conclusions	93
5.7.1	Findings	93
5.7.2	Contributions	94
5.8	Summary	95
6	Investigation on the Acceptance of the Generic Security Template in Health-care Systems - An Industrial Evaluation	96
6.1	Study initiatives	96
6.2	Study design	97
6.2.1	Study objectives	97
6.2.2	Target organisation	98
6.2.3	Participants	98
6.2.4	The study material and pilot test	98
6.3	The study process	99
6.3.1	The consent form	99
6.3.2	The background questionnaire	99
6.3.3	The interview	99
6.3.4	Post-interview questionnaire	100
6.4	Results of the study	102
6.4.1	Background questionnaire	102
6.4.2	Information security management	102
6.4.3	Security incident learning	104
6.4.4	Attitude towards the Generic Security Template	106
6.4.5	Strengths and weaknesses	111
6.4.6	Senarios identified to apply the Generic Security Template	113
6.4.7	Acceptability questionnaire results	113
6.5	Discussion	114
6.6	Summary	120

7	Application of the Generic Security Template to structure a GST Instance from a Specific Security Incident - An Empirical Evaluation	121
7.1	Study objectives	121
7.2	Study design	122
7.2.1	Participants	122
7.2.2	Study material	122
7.2.3	Pilot study	123
7.3	Study execution	123
7.4	Result analysis	123
7.4.1	Background questionnaire	123
7.4.2	Measurement of the results	124
7.4.3	Results for the creation of the instance	125
7.4.4	Results for the post-task questionnaires	127
7.5	External and internal threats	129
7.5.1	Internal validity	129
7.5.2	External validity	129
7.6	Discussion	130
7.7	Summary	130
8	Investigation on the Transferability of Lessons using the Generic Security Template in Healthcare Systems - An Industrial Evaluation	131
8.1	Study design	132
8.1.1	Study objectives	132
8.1.2	Target organisation	132
8.2	The study process	133
8.2.1	Demonstration of the Generic Security Template	133
8.2.2	Execution of the group study - first session	133
8.2.3	Execution of the group study - second session	134
8.3	Execution of the group study - first session	134
8.3.1	Transferring the lessons learned	134
8.3.2	Types of lessons learned and rules of mapping	135
8.3.3	The customised GST instances	138
8.4	Execution of the group study - second session	142
8.4.1	Acceptance of the lessons learned	142
8.4.2	The customised GST instances	144

8.5	Other customisation requirements - multi-view	144
8.6	The revised Generic Security Template Pattern	148
8.7	Discussion	148
8.8	Summary	151
9	Conclusion	153
9.1	Conclusions	153
9.1.1	Dissertation research question 1	154
9.1.2	Dissertation research question 2	155
9.1.3	Dissertation research question 3	156
9.2	Contributions	156
9.3	Limitations and directions for future work	158
9.3.1	Subjective features	158
9.3.2	Scalability	159
9.3.3	Traceability	159
9.3.4	Soundness	159
9.3.5	Industrial evaluation	159
9.4	Closing remarks	160
A	Security Incident Case Studies (Appendix to Chapter 4)	161
A.1	Veterans Affairs (VA) data leakage incident 2006	162
A.2	Veterans Affairs (VA) data leakage incident 2007	163
A.3	Shenzhen data leakage incident 2008	164
A.4	NHS Surrey IT Asset Disposal Incident 2013	165
A.5	Security incidents in the US, China and UK	166
B	The Empirical Experiment (Appendix to Chapter 5)	171
B.1	Participant Consent Form: Usability of GST	172
B.2	VA Data Leakage Incident 2007	174
B.3	Security Standards	179
B.4	Experiment Description	183
B.5	Experiment Tasks	185
B.6	Post-Experiment Questionnaire	189
B.7	Sample Answer	192

C	Industrial Evaluation (Appendix to Chapter 6)	196
C.1	Participant Consent Form: Acceptance of GST	197
C.2	Background Questionnaire	199
C.3	Tutorial - VA Data Leakage Incident 2007	200
C.4	Interview Questions	201
C.5	Acceptability Questions	202
C.6	Background questionnaire results	203
D	The Empirical Experiment (Appendix to Chapter 7)	204
D.1	Instruction	205
D.2	Participant Consent Form	214
D.3	Experiment Task - A case on Credit Card Disposing	216
D.3.1	Appendix 1: Credit Card Disposing Case	217
D.3.2	Appendix 2: Credit Card Disposing Guidelines	218
D.4	Answer Sheets	219
D.5	Post-Experiment Questionnaire	226
E	Industrial Evaluation (Appendix to Chapter 8)	228
E.1	Acceptance of Recommendations: Shenzhen Data Leakage Incident 2008	229
E.2	Acceptance of Recommendations: VA Data Leakage Incident 2007 . .	230
E.3	Acceptance of Recommendations: VA Data Leakage Incident 2006 . .	233
	Bibliography	235

List of Tables

2.1	Description of incident response phases [1–6]	21
3.1	Extension of GSN Pattern Design Notations [7]	47
4.1	Veterans Affairs (VA) data leakage incident 2006	53
4.2	Veterans Affairs (VA) data leakage incident 2007	56
4.3	Shenzhen data leakage incident 2008	60
4.4	NHS Surrey IT Asset Disposal Incident 2013	63
4.5	Time and efforts to create the GST Instances	68
5.1	An exempt of the security issue and recommendation table	75
5.2	The performance of Task 1 using Cross-tabulation by Rater A	81
5.3	Chi-Square Tests performance of Task 1 using Cross-tabulation by Rater A	82
5.4	The performance of Task 1 using Cross-tabulation by Rater B	82
5.5	Chi-Square Tests performance of Task 1 using Cross-tabulation by Rater B	83
5.6	Inter-rater reliability for Task1 Question 1 (Rater A and B)	83
5.7	Inter-rater reliability for Task1 Question 2 (Rater A and B)	83
5.8	Inter-rater reliability for Task1 Question 3 (Rater A and B)	84
5.9	Inter-rater reliability for Task1 Question 4 (Rater A and B)	84
5.10	Inter-rater reliability for Task1 Question 5 (Rater A and B)	84
5.11	Inter-rater reliability for Task1 Question 6 (Rater A and B)	84
5.12	Inter-rater reliability for Task1 Question 7 (Rater A and B)	84
5.13	Landis and Koch-Kappa’s benchmark scale [8]	85
5.14	The performance of Task 2 using Cross-tabulation	85
5.15	Chi-Square Tests performance of Task 2 using Cross-tabulation	86
5.16	Questionnaire sections that belong to Group A and Group B	87

6.1	The strengths of the Generic Security Template	111
6.2	The weaknesses of the Generic Security Template	112
7.1	Average score for different steps of different groups	128
7.2	Average score of different Task Load Index dimentions of different groups	128
7.3	Average score for different evaluation aspects for different groups . . .	129
A.1	Veterans Affairs (VA) dataloss incident 2006	162
A.2	Veterans Affairs (VA) dataloss incident 2007	163
A.3	Shenzhen dataloss incident 2008	164
A.4	NHS Surrey IT Asset Disposal Incident 2013	165
B.1	Experiment task 1	185
B.2	Experiment task 1 (continued)	186
B.3	Experiment task 1 answer	192
B.4	Experiment task 1 answer (continued)	193
C.1	Participant's background	203
D.1	Credit Card Disposing	217
E.1	Acceptance of Recommendations: Shenzhen Data Leakage Incident 2008	229
E.2	Acceptance of Recommendations: VA Data Leakage Incident 2007 . .	230
E.3	Acceptance of Recommendations: VA Data Leakage Incident 2006 . .	233

List of Figures

1.1	An example instance of the Generic Security Template - VA 2007 Data Leakage Incident	6
1.2	Chapter structure	9
2.1	Information Security Management Systems (ISMS) Framework [9] . .	16
2.2	The Incident Response Process [1–5]	22
3.1	CAE argument structure [10]	34
3.2	GSN Notations [11]	35
3.3	An example instance of the Safety Case [11]	39
3.4	Customised GSN Notations	41
3.5	An example instance of the GST - VA 2007 Data Leakage Incident . .	42
3.6	The Generic Security Template Pattern	48
4.1	Instance of the Generic Security Template - VA 2006 data leakage incident	55
4.2	Instance of the Generic Security Template - VA 2007 data leakage incident	59
4.3	Instance of the Generic Security Template - Shenzhen 2008 data leakage incident	62
4.4	Instance of the Generic Security Template - NHS Surrey IT Asset Disposing	65
5.1	An example instance of the GST - VA 2007 data leakage incident . . .	71
5.2	Overall experience of the GST - Group A	90
5.3	Overall experience of the GST - Group B	91
6.1	An example instance of the Generic Security Template - VA 2007 data leakage incident	101

6.2	Customised instance of the Generic Security Template - VA 2007 data leakage incident	109
6.3	Healthcare professionals' attitude towards the acceptability of the GST	114
6.4	Customised instance of the Generic Security Template with lessons learned types - VA 2007 data leakage incident	118
7.1	Goal structure of the Credit Card Disposing Case	124
7.2	Lessons learned of the Credit Card Disposing Case	125
7.3	Mapping lessons learned to the security requirements of the Credit Card Disposing Case	126
7.4	Final Credit Card Disposing Instance	127
8.1	Instance of the Generic Security Template VA 2007 - customised by replacing the security standard	139
8.2	Instance of the Generic Security Template VA 2006 - customised by replacing the security standard	140
8.3	Instance of the Generic Security Template Shenzhen	141
8.4	Instance of the Generic Security Template Shenzhen 2008 - customised by implementation types	145
8.5	Instance of the Generic Security Template VA 2007 - customised by implementation types	146
8.6	Instance of the Generic Security Template VA 2006 - customised by implementation types	147
8.7	Instance of the Generic Security Template Shenzhen - customised after adding the multi-view identifiers	149
8.8	The adjusted Generic Security Template Pattern after a series of customisation	150
B.1	Generic Security Template - VA data leakage 2007	184
C.1	Generic Security Template - VA data leakage 2007	200
D.1	Credit Card Disposing Guidelines	218

Chapter 1

Introduction

This chapter introduces the research background and formulates the dissertation statement and research questions. It is divided into three sections. Section 1.1 introduces the current status on information security management, security incident handling and information security incident learning. Section 1.2 defines the dissertation statement and research questions. Section 3.3 introduces the structure of this dissertation and provides an overview of each chapter.

1.1 Background

1.1.1 Information security incident

“The Information Commissioner’s Office (ICO) has issued NHS Surrey with a monetary penalty of £200,000 after more than 3,000 patient records were found on a second hand computer bought through an online auction site. The sensitive information was inadvertently left on the computer and sold by a data destruction company employed by NHS Surrey since March 2010 to wipe and destroy their old computer equipments.” [12].

Such an incident may result in financial losses and legal issues, and affect the organisations’ reputation and customer confidence [13]. Security incidents happened in healthcare organisations across the world such as Veterans Affairs’ data leakage incidents [14, 15] in North American and Shenzhen hospital’s data leakage incident [16] in China. However, those incidents are just the tip of iceberg. Industry reports indicate that the number of security incidents happened in healthcare organisation is increasing. Symantec reports that the healthcare industry accounted for 36% of the total security incident breaches in 2012 [17]. At 44%, the healthcare industry contin-

ues to be the sector responsible for the largest percentage of disclosed data breaches by industry in 2013 [18]. Symantec captured this data from more than 157 countries through a variety of Symantec products and services such as the Symantec Probe Network, Symantec.cloud, Norton consumer products, and other third-party data sources [18].

A patient's medical record is a collection of personal information including "identification, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income, and physicians' subjective assessments of personality and mental state among others" [19, 20]. Healthcare information privacy and security have been a primary concern of the public [21–25]. Waegemann claimed that the disclosure of a patient's medical record could ruin or damage an individual's career, and result in dismissal from work, loss of health insurance and financial loss [26].

Data leakage incidents can cause financial loss to healthcare organisations. Healthcare organisations will be fined if they fail to protect patients' personal information. For instance, the healthcare organisations in UK were fined hundreds of thousands pounds following data breaches affecting thousands of patients and staff [27–29]. Although it is a small amount comparing to the total budget of UK healthcare organisations which is over hundreds of billions pounds, this situation can become worse if no actions taken to reduce such security incidents [30].

1.1.2 Legislative and government initiatives

The new European General Data Protection Regulation [31], extends the scope of the Data Protection Directive (Directive 95/46/EC) to all foreign organisations processing data of European Union residents. It comes with a strict data protection compliance regime that organisations can be fined up to 2% of worldwide turnover, for example, in the case of severe data protection incidents and failure to report a personal data breach to the supervisory authority. Organisations are under a legal obligation to strengthen their security mechanisms to prevent incidents. There are also government initiatives to enhance the sharing of security incidents. For example, the UK has launched the Cyber Security Information Sharing Partnership (CISP) to help government and industry on cyber security threats. The partnership includes the introduction of a secure virtual "collaboration environment" where government and industry partners can exchange information on threats and vulnerabilities in real time [32]. There is a need to promote

incident knowledge exchanging by providing the ability to analyse and redistribute this knowledge effectively [32].

1.1.3 Information Security Management Systems (ISMS)

Information Security Management Systems (ISMS) can be defined as management systems used for establishing and maintaining a secure information environment [33]. The objective is to “implement the appropriate measures in order to eliminate or minimise the impact that various security related threats and vulnerabilities might have on an organisation” [9]. Current research has provided security controls for preventing information security threats and vulnerabilities, including technical protection (e.g. anti-virus software and firewalls) and management protection (e.g. security training, security standards and guidelines). However, the main stream of those researches has placed less emphasis on the lessons learned from the security incidents as a resource to improve the implementation of security controls. The key learning notes are not effectively fed back into management structure, security policies and procedures [5]. There is a need to effectively communicate learning from security incidents to inform improvements in ISMS.

1.1.4 Security incident response

Security incident response is an important part of ISMS [34]. It can be defined as “the process that aims to minimise the damage from security incidents and malfunctions, and monitors and learns from such incidents” [1, 2]. There are well-documented methodologies such as the SANS [3, 4] and NIST SP800-61 models [35, 36] that divide this process into several distinct phases to handle and respond to an incident, including preparation, identification, containment, eradication, recovery and follow-up [2]. Incident response process prepares preventative measures, identifies an incident, contains the incident, removes the incident, recovers the systems and then conducts a post-incident review to document and disseminate key learning notes, which is usually called a “feedback” or “follow-up” phase.

A “feedback” or “follow-up” phase is an indispensable stage of the security incident response process according to NIST [35, 36] and SANS [3, 4]. A key activity in the incident response process is the capacity to learn from the errors or mistakes made throughout the incident handling process, to learn about the effectiveness of security policies, procedures, technical processes and to feed this knowledge back into the in-

formation security management process [3, 36]. Current research has realised the importance to learn from past security incidents [6, 37–40]. However, incident response often focuses on solving the direct cause of the incident, rather than investigating the in-depth cause which is often not a technical problem (e.g. firewall not properly configured) but a management problem (e.g. not having a policy for configuring firewall) [6]. This imbalanced focus has resulted in the loss of opportunities to investigate why a potential incident is not adequately covered by the security requirements, that may lead to further improvements of the security requirements and may prevent future incidents [6]. Firesmith defines security requirements as “a quality requirement that specifies a required amount of security in terms of a system-specific criterion and a minimum level that is necessary to meet one or more security policies”[41]. For example, a security requirement related to access control cited from ISO 27002 can be “Ensuring that information is accessible only to those authorised to have access”[42].

1.1.5 Current methods in sharing the lessons learned

There have been several initiatives in supporting security incidents sharing and exchanging. For example, the European Network and Information Security Agency (ENISA) requests member states to report security incidents to enable the exchange of lessons from incidents. In the United States, the nation’s Healthcare and Public Health Information Sharing and Analysis Centre (NH-ISAC), has provided a platform for sharing and exchanging lessons learned from security incidents in healthcare organisations [43]. However, their work was not concerned with providing a mechanism for conveying key details effectively.

Traditional ways to disseminate information about an incident include a series of formal reports, emails, newsletters, meetings and presentations to management [3, 36]. Meetings are held and communicative notes are gathered to address responses, disagreements, suggestions and additions to security requirements and the incident procedures [3]. Emails, newsletters, meetings and presentations to management contain less information comparing to the formal post-incident reports. Post-incident reports document information obtained throughout the security incident investigation process. Example post-incident reports include the VA data leakage incidents [14, 15] from the US, the NHS IT Asset disposal incident [44] from UK. They provide a reference that can be used to assist in handling similar incidents [35, 36]. Contents include the causes of the incident, the recommendations on remediation, the security requirements

violated and improvements on procedures. Although this information is inter-related, details can be scattered throughout a report (Appendix A.5). This makes it difficult for readers to understand how the recommendations are brought together to support different security requirements [45]. This problem has been compounded by usually lengthy written security incident reports, which can be hundred of pages. There is a need for the conversion of the textual information into a learning document, that can easily communicate security lessons into the ISMS [6].

Traditional ways to disseminate lessons learned are based on text approach. The linear format of a text can obscure relationships among concepts and discourage readers from integrating information across ideas [46]. Graphical diagrams can serve this purpose, as it can communicate both individual elements of information and relationships between them.

In this dissertation, we propose a novel diagramming approach, the Generic Security Template, aiming to provide a mechanism to feed back the lessons learned to the ISMS. Rather than developing another novel security notation with an uncertain pedigree, we have extended the application of the existing Goal Structuring Notation (GSN) [7] to support the exchange of lessons learned in the aftermath of data leakage. The objective is to enhance existing techniques used to share lessons from security incidents. Bloomfield claimed that GSN had become the dominant approach in the UK defence sector [10], and it is increasingly being used in safety-critical industries to improve the structure, rigor, and clarity of design requirements [47, 48]. The same approach has more recently been extended to document security requirements [45, 49–52]. We believe this approach can be adapted to effectively communicating security lessons into the ISMS. It is important to note that this newly proposed approach is not intended to replace any of the existing lessons learned dissemination methods. It provides a new way to feed back the lessons learned from the security incidents to the ISMS. Section 1.2 outlines the dissertation statement.

1.2 Dissertation statement

1.2.1 Hypothesis

The Goal Structuring Notations (GSN) can be used to depict the lessons learned from security incidents and map them to the security requirements for an Information Security Management System. We define the resulting graphical overview as the Generic

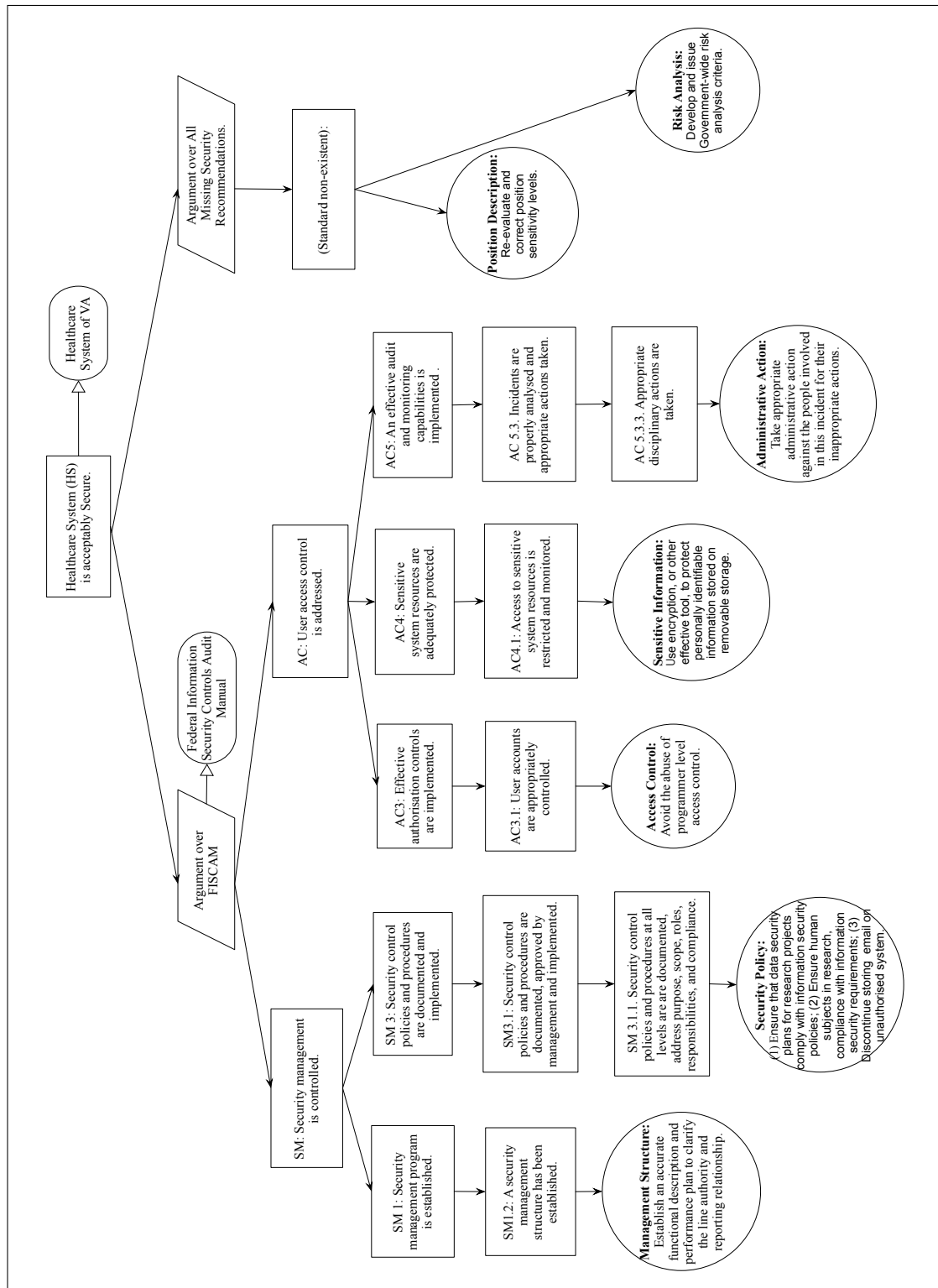


Figure 1.1: An example instance of the Generic Security Template - VA 2007 Data Leakage Incident

Security Template (GST). We argue that the GST can assist users to identify the lessons learned from security incidents and can be applied to structure the insights derived from specific security incident. The GST is acceptable in a healthcare organisation and can be used to feed back the lessons learned to an Information Security Management Systems in healthcare.

1.2.2 Definitions

A Generic Security Template (GST), can be defined as “a semi-structured body of lessons identified from security incidents that can support identification of security requirements of the Information Security Management Systems (ISMS)”. It presents the lessons learned in a structured manner by mapping them to the security requirements of the ISMS.

A security incident, is defined as “a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices” [53]. In this dissertation hypothesis, we focus on security incidents that are publicly reported in healthcare systems.

Lessons learned, are defined as the knowledge or understanding gained by experience [54]. In this dissertation, it refers to (1) security issues (the causes of a security incident in confidentiality); and (2) security recommendations (intended to avoid any recurrence).

Security requirements of an ISMS, are presented in the form of a common security standard or guideline applied to the organisation where the security incident happened.

Generic, is defined as “characteristic of or relating to a class or group of things; not specific”. In this thesis, Generic Security Templates are intended to be applicable across different classes of organisation and not specifically to the place where an incident occurred.

The GST is a theoretical model that maps the lessons learned to the security requirements. The Generic Security Template that describes a specific security incident is defined as a GST instance. Figure 1.1 provides an example instance of the GST. It is based on a report into the data leakage of personal information about 250,000 veterans and over 1.3 million medical providers by the US Veterans Affairs Administration (VA) [15]. The leaf nodes in this diagram are used to gather the lessons learned that were intended to avoid future incidents. The internal nodes are used to show how each of these findings supports higher level goals and sub-goals intended to ensure

that systems meet an acceptable level of security, defined in terms of the US Governments Federal Information System Controls Audit Manual (FISCAM) [55], a security guideline applied to the VA. More details will be elaborated in subsequent chapters.

1.2.3 Research questions

The following research questions are formulated to support the dissertation statement.

1. Can the GST be used to depict lessons learned from security incidents and map them to the security requirements for an Information Security Management System?
2. Can the GST be used to better assist users to identify the lessons learned from security incidents in comparison to traditional free-text approaches?
3. Can the GST be accepted and used to feed back the lessons learned to an Information Security Management Systems in healthcare?

1.3 Dissertation structure

The objective of the dissertation is to propose an approach to feed back the security lessons to the Information Security Management Systems in healthcare organisations. Figure 1.2 presents an overview of the chapters and their relational structure.

Chapter 2 presents a theoretical framework on which the dissertation is based through a comprehensive survey of relevant research and current literature. It includes Information Security Management Systems (ISMS), security incident response lifecycle, lessons learned from the security incidents and how the lessons learned are related to the ISMS and security incident response lifecycle. The context of the research is then outlined, where a focus is placed on feeding back the lessons learned from security incidents to the ISMS.

Chapter 3 proposes the Generic Security Template. It introduces the basis of the Generic Security Template, including assurance cases, the graphical Goal Structuring Notations (GSN), and outlines the processes to create instances of the Generic Security Template.

Chapter 4 answers research question 1 by conducting four security incidents case studies from the US, UK and China. It tests the suitability of the Generic Security Template by producing four instances of the Generic Security Template following the creation process presented in Chapter 3.

Chapter 5 answers research question 2 by empirically evaluating the usability of the

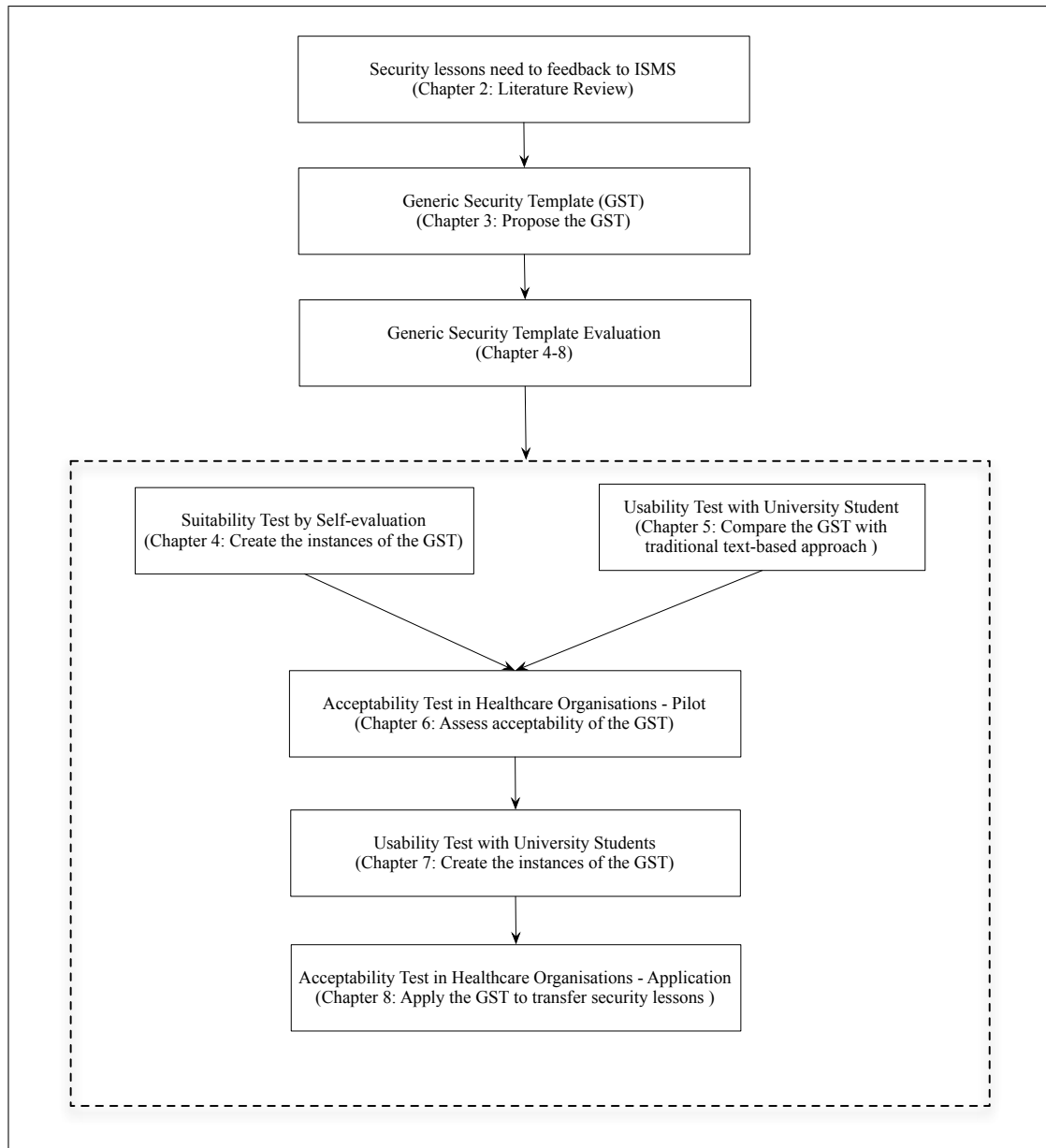


Figure 1.2: Chapter structure

Generic Security Template in assisting the identification of the lessons learned from the security incidents compared to the traditional pure free-text approach. In particular, its usability is evaluated in terms of accuracy, efficiency and ease of use to identify the lessons learned from security incidents. The results show that it can help improving the accuracy and reducing the mental effort in identifying lessons learned from security incident reports.

Chapter 6 answers research question 3 by evaluating the acceptability of the Generic Security Template with people working in healthcare. The objective is to assess people's general attitude towards this approach. It identifies strengths and weaknesses of the Generic Security Template, and appropriate scenarios in which the Generic Security Template can be applied to fit the needs of the organisation.

Chapter 7 synthesises the feedback from Chapter 4, 5, 6 into the improvements of the Generic Security Template and evaluates the improved Generic Security Template by conducting an empirical study with university students with a computer science background. The results show that users with a computer science background can structure the insights derived from a security incident using the Generic Security Template. This further answers research question 1 that the Generic Security Templates can be used for structuring the lessons learned from the security incidents.

Chapter 8 further answers research question 3 through several in-depth industrial case studies to examine the Generic Security Template's capability to feed back the security lessons to the ISMS. In particular, we use the security incidents from different countries to find out how lessons learned can be transferred to a representative healthcare organisation in China. The findings show that, by using the GST, lessons identified from security incidents from one healthcare organisation in a specific country can be transferred to another and can indeed inform improvements of the ISMS.

Chapter 9 summarises the conclusions, contributions, limitations and lays down the foundation for future work.

Chapter 2

Review of Literature

This chapter presents the theoretical framework on which the dissertation is based through a comprehensive survey of relevant research and current literature. It introduces Information Security Management Systems (ISMS), security incident response lifecycle, incident learning and how the incident learning is shared and exchanged using current dissemination methods. This chapter finally outlines the context of the research, where a focus is placed on feeding back the lessons learned from security incidents to ISMS. This chapter is divided into the following sections.

Section 2.1 introduces information security and the healthcare information security. It includes concepts of information security, security threats, vulnerabilities, and countermeasures. Section 2.2 introduces Information Security Management Systems (ISMS). It includes the definition of ISMS, the ISMS framework and current initiatives of the ISMS including security standards, guidelines and best practices. Section 2.3 introduces information security incident response and handling related literatures, which is a part of ISMS. It includes the definition of security incident and the security incident response lifecycle. Section 2.4 introduces related work on incident learning which is an important part of the incident response lifecycle, as well as industrial and government initiatives in incident learning. Section 2.5 introduces current methods in sharing lessons learned from the security incidents and identifies the problems with current methods. Section 2.6 outlines the context of this research, where we identify the theoretical and industrial requirements as the motivations of this dissertation.

2.1 Information security

2.1.1 Definition of information security

Information Security refers to “the preservation of confidentiality, integrity and availability (CIA) of information” [34]. This definition is consistent with the work by Pfleeger [56], Denning [57] and Gollmann [58]. Availability is “the property being accessible and usable upon demand by an authorised entity”. Confidentiality is “the property that information is not made available or disclosed to unauthorised individuals, entities or processes”. Integrity is “the property of safeguarding the accuracy and completeness of asset” [34]. However, Dhillon suggested that the CIA principles are not enough to address information security [59]. There are extra principles, such as responsibility, integrity, trust and ethicality (RITE). ISO 27001 also introduces authenticity, accountability, non-repudiation and reliability. Organisations need to consider all those aspects to ensure a secure environment for their information assets. However, achieving those objectives is non-trivial because security breaches stem from a variety of sources and channels. These include but are not limited to careless or unaware employees, out-dated security controls, frauds, malware, espionage, phishing, unauthorised access, spam, cyber-attacks and vulnerabilities [60].

2.1.2 Security threats, vulnerabilities, and countermeasures

A security threat is “any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service” [61]. Security threats are unexpected and have the potential to cause an unwanted incident that can negatively impact a system or organisation.

A vulnerability refers to any weakness in computer software or hardware systems that can be accidentally triggered or intentionally exploited [62]. Vulnerabilities open the system to attacks that have the potential to violate the system’s intended secure behaviour. Currently, the number of the security vulnerabilities is still increasing. For example, the United States’ national vulnerability database [63] lists over 40.000 security problems at an increasing rate of 13 vulnerabilities per day.

A countermeasure refers to any security service that can reduce security threats and vulnerabilities by minimising the harm it can cause. It is a procedure or mechanism

that reduces the probability that a specific vulnerability will be exploited, or reduces the damage that results from a specific exploitation. Examples of countermeasures include both management means such as security policy, standards, guidelines, security awareness training, and technical means such as built-in or add-on security products, access control mechanisms, and encryption methods [62].

2.1.3 Information security in healthcare systems

Electronic medical records (EMR) are gradually replacing the traditional paper-based record as it can provide many benefits such as reducing the cost and enhancing the quality of healthcare service delivery [64–66]. The use of the EMR also faces great challenges as it expands the volume of health information accessible by both authorised and unauthorised users. The spread of electronic medical records raises privacy concerns [64, 67].

Health information is considered to be more sensitive than other types of personal information [68, 69]. Studies conducted in different countries reveal people's concern about health information security and privacy. For example, in the United States, individuals are required to execute millions of compelled authorisations for the disclosures of health information each year for various purposes such as employment and insurance. There are no restrictions on the scope of the released information [70]. In the studies conducted in Denmark [71], New Zealand [24], Australia [72] and China [73], individuals are also found to be concerned with the sharing of their health information.

The threats of the health information security can be external or internal [74]. External threats include viruses and spyware attacks, hackers, and intruders in premises. Internal threats include various types of employee behaviour such as ignorance, curiosity, recklessness, inadequate behaviour, and abuse of password [75]. The United States National Research Council classified the healthcare organisational threats into five levels, according to increasing sophistication [67],

- Accidental disclosure, patient information is unintentionally disclosed to others by careless healthcare personnel (e.g. e-mail message sent to wrong person);
- Insider curiosity, an insider with data-access privilege access a patient's records for personal interest and purpose, (e.g. concerns of well beings of their friends);
- Data breach by insider, insiders access and transmit the patient's information to outsiders for money or personal revenge, etc;

- Data breach by outsider with physical intrusion, an outsider illegally intrudes the physical facility and gains access to the system.
- Unauthorised access, an outsider intrudes into a healthcare organisation's network from the outside to gain access to patient information or attack the system.

Reviews of literature [20, 69, 76] show that security technologies applied in healthcare organisations are largely from cryptographic and distributed systems research, including both technical means such as health data encryption [77, 78], access control [79, 79, 80], secure data exchanging between organisations [81, 82] and management means such as compliance of the security standards or policies [83, 84], audit logs analysis [85, 86], security training [83, 87, 88] and so on. Those support five main principals of healthcare information security [89, 90],

- Availability and integrity, ensure that the information is accurate and up-to-date and available at appropriate places;
- Accountability, ensure that health care providers are accounted for their use of information, based on documented needs and rights;
- Perimeter definition, control the boundaries of trusted access to the information system, both physically and logically;
- Role/need-limited access, enable access for personnel only to information essential to the performance of their jobs, and limit any temptation to access information beyond the needs;
- Comprehensibility and control, ensure the stakeholders of the medical record including record owners, data stewards, and patients can understand and have effective control over appropriate aspects of information security and access.

Effective countermeasures including both management and technical security controls are required to prevent or eliminate threats, or vulnerabilities, and minimise the harm they can cause. The objective of information security management is to “implement appropriate measurements in order to eliminate or minimise the impact that various security related threats and vulnerabilities might have on an organisation” [9]. The next section elaborates on the Information Security Management Systems (ISMS).

2.2 Information Security Management Systems (ISMS)

2.2.1 Information Security Management Systems

There has not been a canonical definition of Information Security Management Systems (ISMS). The world was introduced to the formal concept of ISMS during the 1990s with the development and introduction of the British Standard BS-7799 [91], which was incorporated in the ISO 27000 series. Eloff defines an Information Security Management System as a management system used for establishing and maintaining a secure information environment [33]. Information Security Management Systems incorporate the typical “Plan-Do-Check-Act” (PDCA) cycle, proposed by Deming [92, 93]. The main tasks in the “Plan” phase is to design the ISMS, assess information security risks and select appropriate controls. The security controls are then implemented in the “Do” phase. The “Check” phase reviews and evaluates the performance (efficiency and effectiveness) of the ISMS. In the “Act” phase, remedial actions are taken and security lessons are documented. This data can be put back into the risk assessment process in the “Plan” phase, ultimately leading to the improvements of the ISMS.

2.2.2 Information Security Management Systems framework

ENISA outlines the ISMS framework as shown in Figure 2.1. The development of an ISMS framework includes six steps, definition of security policy, definition of ISMS scope, risk assessment (as part of risk management), risk management, selection of appropriate controls, and statement of applicability [9]. This is consistent with the requirements in the ISO 27000 series [34, 42].

The definition of a security policy and the scope of the ISMS, are higher-level management strategies. In healthcare, regulations and policies have been proposed in different countries, such as Health Insurance Portability and Accountability Act (HIPAA) [94] in the US, the Data Protection Act [95] in the UK and the Personal Information Protection Act [96] in China. Risk management is a process to “transform” the security standards, guidelines of security policy, the targets, and objectives of ISMS into specific plans for the implementation of controls and mechanisms that aims to minimise threats and vulnerabilities. Security risk management (SRM) is a continuous process to prioritise information system security risk, implement and monitor security controls (i.e., countermeasures, safeguards) [13, 36]. It synthesises the strategies, policies, ac-

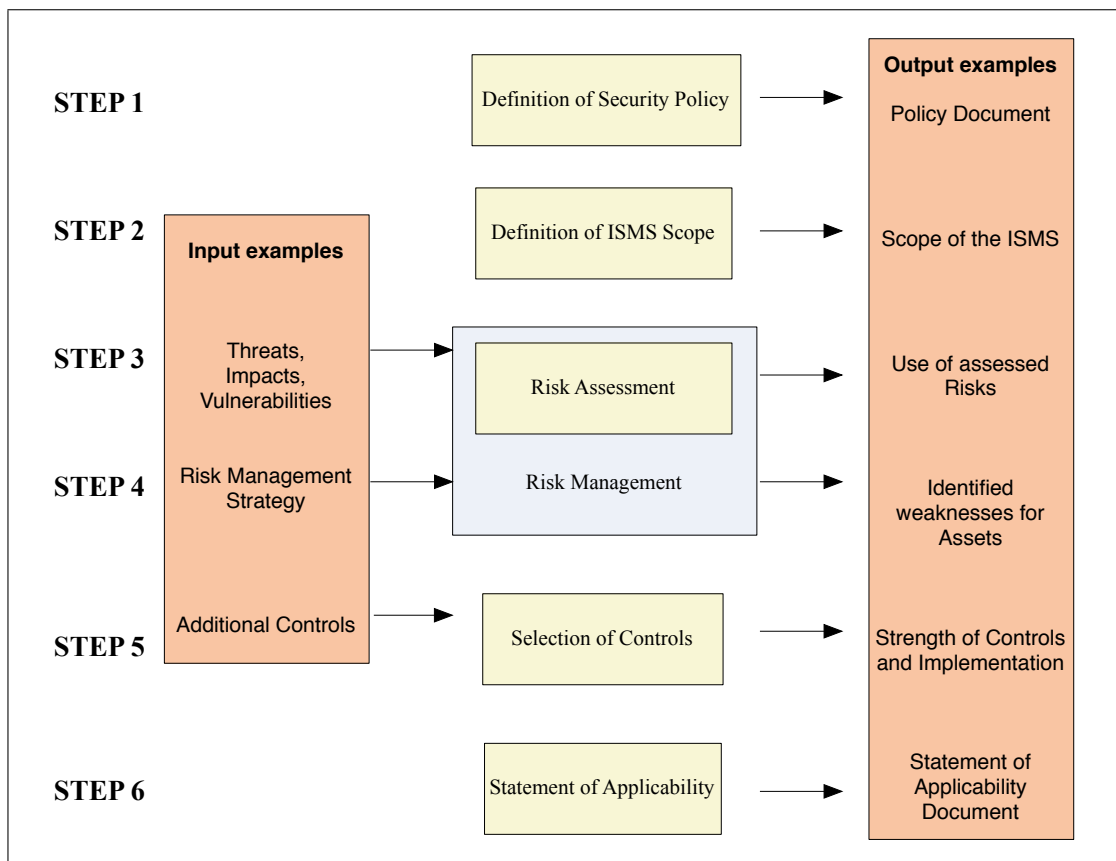


Figure 2.1: Information Security Management Systems (ISMS) Framework [9]

tivities, procedures, and people used to manage security risk, and is expected to result in a system of controls that collectively protect information systems security [34, 42]. Appropriate controls are then selected and mapped to the identified risks. The sources of the controls are mainly from existing sets of controls or mechanisms, included in information security standards (e.g. ISO 27001) and guidelines, or a combination or adaptation of proposed controls to the specific organisational requirements. Section 2.2.3 reviews these controls.

2.2.3 Security standards and guidelines

There have been a number of initiatives to contribute to the ISMS. Several private and government organisations developed guidelines to ensure that an adequate level of security is achieved and best practices adopted in an organisation, such as ISO27001, BS7799, CMMI [97], FISCAM [55], GB/T22239 [98], ITIL [99], Common Criteria [100], SecUML [101] and COBIT [102]. Security standards provide a detailed level of mandatory controls to support the enforcement of information security policies. Secu-

rity guidelines consist of recommended controls and best practices to support security standards or serve as a reference when no applicable standards are available. The following sections introduce some example standards or guidelines.

The Federal Information System Controls Audit Manual (FISCAM) provides best practices on security control techniques and audit procedures [55]. It is consistent with the Federal Information Security Management Act (FISMA) [103] and has incorporated NIST Standards such as NIST SP 800-53 [104], NIST SP 800-100 [105]. FISMA defines a framework for managing information security that must be followed for all information systems operated by a U.S. federal government agency. The FISCAM can be used as the basis for a FISMA evaluation and has provided different levels of security requirements for evaluating general security controls. FISCAM includes general controls categories such as security management, access controls, configuration management, segregation of duties and contingency planning. For each of those general control areas, it identifies several critical elements that are essential security requirements for establishing adequate security controls.

In the Chinese standard, GB/T22239 (Information security technology - Baseline for classified protection of information system), there are four classified security levels to ensure information security [98]. Baseline security requirements are provided for different levels,

- The first level requires the ISMS to protect the system from malicious attacks from individual or small scale threats with few resources; to resist the general natural disasters or other harms caused to critical resources; and to recover at least part of the functions after the system is compromised or damaged.
- The second level requires the ISMS to protect the system from malicious attacks from small organisations or small scale threats with few resources; to resist the general natural disasters or other harms caused to critical resources; to detect important security vulnerabilities and security events; and to recover at least part of the functions after the system is compromised or damaged.
- The third level requires the ISMS to protect the system from malicious attacks launched by organised groups or threats with abundant resources by following unified security strategy; to resist severe natural disasters or other harms caused to critical resources; to detect important security vulnerabilities and security events; and to recover most of the functions after the system is compromised or damaged.

- The fourth level requires the ISMS to protect the system from malicious attacks launched by state-level threats or from hostile organisations by following unified security strategy; to resist severe natural disasters or other harms caused to critical resources; to detect important security vulnerabilities and security events; and to recover almost all the functions after the system is compromised or damaged.

Organisations are required to comply with the GB/T22239, by achieving a certain security level. For example, the guidance of the health industry information security level protection issued by the Ministry of Health of the People's Republic of China requires that, health information systems and related units should be self-examined in accordance with GB/T22239. In particular, the tertiary (highest level) hospital needs to achieve at least the third level of the GB/T22239 [106].

2.2.4 Strengths and weaknesses of security standards/guidelines

Organisations can potentially benefit from standards/guidelines in two ways [107, 108]. The first is to ensure the development of a strong, consistent and structured strategy to protect information security. Security standard/guidelines provide best practice and recommend security requirements that the organisation needs to meet and it is a good starting point for shaping information security management strategy [107, 109]. The second is to demonstrate to the staff, customers and trading partners that the organisation has taken security seriously by following international best practices. Gomes introduced the ISO 27002 for implementing four security controls (Asset Management, Physical and Environmental Security, Communications & Operations Management, Access Control) in a data center infrastructure of Hospital S. Sebastiao in Portugal [110]. The application of this framework was reported to be successful, justified by the well accomplishment of those four security controls [110]. Wiander analysed the implementation experiences of four organisations that have implemented ISO/IEC 17799 (2005). The results suggest that the standard served the needs of the enterprises and its intended usage correlated well with organisations' practice [111].

Siponen criticised the basis of the security standards/guidelines. He argues that many are only based on personal observation and not universally valid [112]. The standards/guidelines are validated by appealing to common practise and authority only, which is not a sound basis for international use [113]. However, information security standards/guidelines can serve as information security management library for prac-

tioners [113]. Practitioners would benefit from in-depth practical experiences and lessons learned on how the objectives of security standards/guidelines are met in organisations where they are applied [113].

2.2.5 Security requirement modelling

Security standards provide security requirements that are based on best practices. As is mentioned, some organisations adopted security requirements from security standard directly. As an alternative, organisations can model their own security requirements by using security requirement modeling methods such as Common Criteria (CC) [114] and SecUML [101, 115]. The Common Criteria (CC) is an international standard (ISO/IEC 15408). It allows the security experts to elicit security requirements and specify security attributes of their own products. The SecUML [101, 115] is a modelling language that defines abstract syntax for annotating UML diagrams with information relevant to access control. The meta-model consists data types like users, roles, objects, operations and permissions and was found to be able to ease the expression of access control requirements during analysis and design [101].

2.2.6 ISMS and incident learning

As mentioned, ISMS incorporate the typical “Plan-Do-Check-Act” (PDCA) cycle. Incident learning is viewed as a resource that can be used to improve procedures, policies, and implementing new controls [5], which involves every step of the ISMS. However, incident learning is not given much attention in the research literature [5]. An exploratory case study conducted in a large global financial services organisation shows that the practice of incident response frequently do not result in the improvements of strategic security processes such as policy development and risk assessment. The key learning notes are not effectively fed back into security processes, management structure, policies, procedures and risk assessment [6]. There is a gap between the learning of security incident and the ISMS, to translate the learning to inform improvements of the ISMS. Sections 2.3 examines incident learning from the perspective of security incident management lifecycle.

2.3 Security incident management

2.3.1 Security incident

Krause defines a security incident as “any act or circumstance that involves classified information that deviates from the requirements of governing security publications ” [116]. An information security incident occurs when the confidentiality, integrity and availability of an information asset are directly or indirectly attacked. Those attacks include but are not limited to malicious software, the loss of sensitive information, the loss of power and supporting utilities. Such incidents result in financial losses and legal issues. They affect the organisations’ reputation and customer confidence [13].

2.3.2 Security incident response lifecycle

SANS [3, 4] and NIST SP800-61 [35, 36] have provided well-structured methods for security incident response. The methods are similar in responding and handling security incidents that typically incorporate initial preparatory phases, the detection and containment of incidents, recovery from incidents and a post-incident follow-up phase. Specifically, the SANS method features six steps: preparation, identification, containment, eradication, recovery and lessons learned [3, 4]. The NIST 800-61 model defines a security incident response and handling lifecycle including four steps: preparation, detection and analysis, containment, eradication and recovery and post-incident activities [35, 36]. Figure 2.2 illustrates a synthesis of this incident response process. Table 2.1 describes each phase of the incident response process in further details.

Although standard incident response processes include a “post-incident” or “follow-up” phase where lessons are to be learned, incident response has focused on technical aspects over incident learning [5]. Reflection on incident response typically does not leverage opportunities to learn about the effectiveness of security procedures, controls, training and policies in order to improve the organisation’s security management capabilities [37, 38]. Section 2.4 further discusses and elaborates on the “follow-up” phase, where learning and incident dissemination occurs.

Table 2.1: Description of incident response phases [1–6]

Phase	Description
Preparation	This phase prepares the resources and tools including incident communication facilities, incident analysis and mitigation tools to handle incidents. This phase also prevents the incident for securing networks, systems, and applications. Main practices include risk assessment, user awareness training, etc.
Identification	This phase detects and analyses security incident. Main practices include incident documentation, prioritisation and notification.
Containment	This phase contains the incident before it overwhelms resources or increases damage. Main practices include choosing a containment strategy, gathering evidence and identifying attack hosts.
Eradication	This phase remedies consequences of the incident based on the information gathered on the incident. Main practices include deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. In this phase, security engineers focus on technical aspects to mitigate security issues.
Recovery	This phase restores systems to normal operation. Main practices include confirming that the systems are functioning normally, and remediating vulnerabilities to prevent similar incidents.
Follow up	This phase allows the organisation to learn lessons and improve their information security management process. Main practices include the completion of incident reports, disseminating of lessons learned to the stakeholders of this incident as well as the improvements of information security management and incident response process from managerial perspectives.

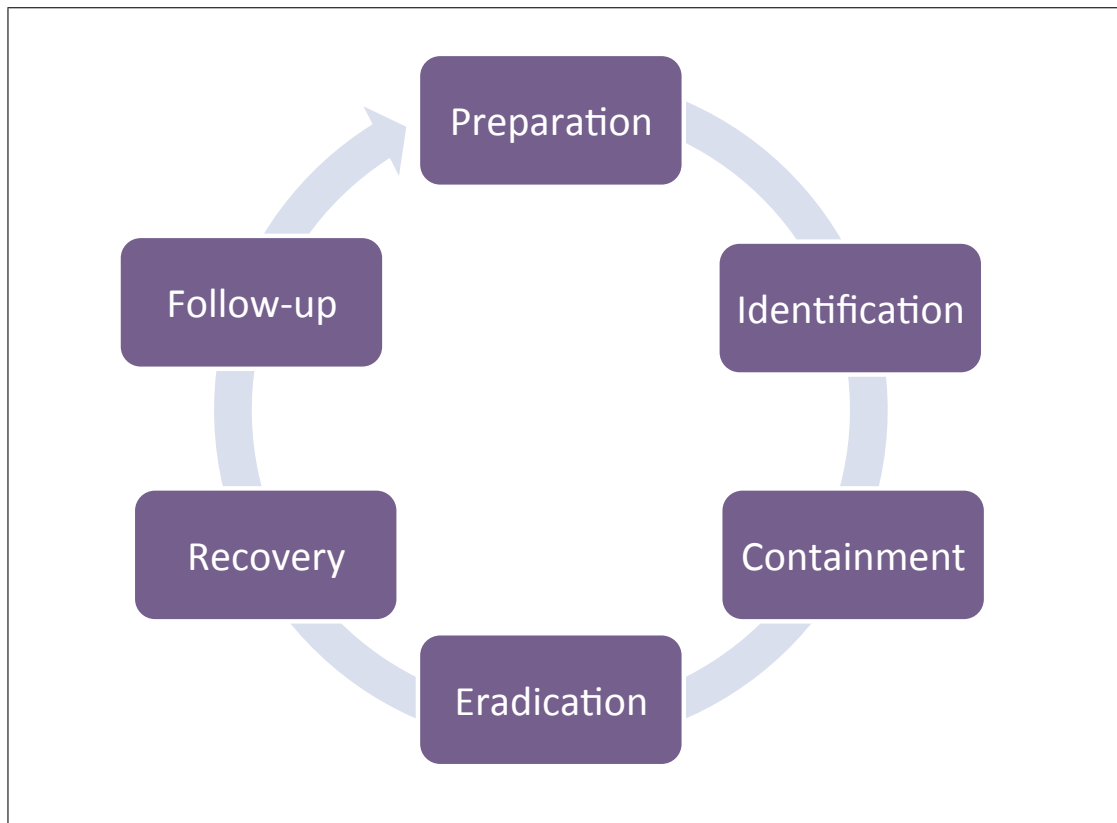


Figure 2.2: The Incident Response Process [1–5]

2.4 Incident learning

2.4.1 Post-incident activities

Incident learning is usually conducted through a series of formal reports, meetings and presentations to management in follow-up phase [3, 36]. These lessons learned should feed back relevant knowledge and changes into the security management process to inform the creation of further reference material on how to respond to similar incidents [36]. In particular, such activities feed information back to the preparedness phase to determine if additional tools, increased security budgets, improved training programs and alterations to the incident response procedures are required.

Some organisations have failed to learn the lessons from security incidents [37, 38, 117]. Muhren describes how “considerable opportunities remain unseized” [117]. Organisations are reluctant to conduct post-incident reviews, as they are costly, challenging and require great expertise to conduct [118]. However, the learning gathered throughout incident handling will be lost unless at least some review activities attempted. Existing work on cost-benefit trade off can help decide IT security invest-

ments [119–122].

2.4.2 Imbalanced focus in security incident learning

There are incident response literatures stressing the importance on the post-incident learning [35], however, compared to the level of details devoted to the technical aspects, few researches provide the details on how this activity should be conducted [6]. Tan et al. have found that many organisations are not prepared to gather and learn the lessons from security incidents. They usually choose to resume service as their priority [123]. More research is required to investigate how organisations can effectively learn from the incident response process. There is a need for the organisations to document, review, and present the lessons and integrate them back into the information security management process for future improvements [5, 6]. However, it is not clear as to how organisations can effectively learn and respond to this information [5]. Section 2.5 elaborates on recent initiatives to incident learning.

2.4.3 Current initiatives in incident learning

2.4.3.1 Legislative requirements

There are legislative requirements to report security incidents. In the US, federal law requires federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS) [53]. In China, there are regulations that ask organisations or enterprises to report incidents as they occur or when they are discovered. It is required that internet platform provider and search engineers (such as, Yahoo!, Google, and Baidu), internet database connector, and the China Internet Network Information Centre (CNNIC) and its service institute should monitor and report incidents to the Bureau of Communication Security with copy to CNCERT/CC (Article 7). Article 63-65 of the Emergency Response Law of the People's Republic of China states that, an organisation that failed to report or which makes a false report will suffer from administrative sanctions which may include license suspension or revocation [124].

The European Commission, in collaboration with the EU Member States, has undertaken a number of legislative initiatives aiming to further improve transparency about incidents. For example, the new European General Data Protection Regulation [31] comes with a strict data protection compliance regime that organisations can be

fined up to 2% worldwide turnover if they failed to prevent a severe data incident or failed to report a personal data breach to the supervisory authority. Another important step is the proposed Cyber Security Strategy [125], which emphasizes incident reporting and the importance of exchange across the EU about incidents.

2.4.3.2 Government initiatives

The UK government has also begun to support the sharing and exchanging of the lessons from security incidents. For example, a Cyber Security Information Sharing Partnership (CISP) program has been launched by the UK government. It aims to help government and industry share information and intelligence on cyber security threats. The partnership introduces a secure virtual “collaboration environment” where government and industry partners can exchange information on threats and vulnerabilities in real time [32]. This is a need to promote incident knowledge exchanging by providing the ability to analyse and redistribute this knowledge effectively [32], that can ultimately strengthen UK’s cyber security knowledge, skills and capability [126].

2.5 Sharing of the lessons learned

2.5.1 Lessons learned sharing through agent organisations

As is mentioned, there have been some initiatives in supporting security incident sharing and exchanging. The ENISA requests the member states to report the security incidents to enable exchange of security lessons. They have used a single set of security measures and a common reporting template allowing for collection and analysis. ENISA has published an analysis of the 51 severe incidents in September 2012 [127]. This report provides examples of incidents, the analysis of the impact per service and per root causes, and then a detailed analysis of the root causes for sharing. According to ENISA, incident sharing contributes to ensure: “access to a wide pool of expertise about such breaches or losses; the analysis of threats and vulnerabilities; the identification of good practice, based on lessons learned in the incident management process” [128].

In the US, the nation’s Healthcare and Public Health Information Sharing and Analysis Centre (NH-ISAC), has provided a platform for sharing and exchanging lessons learned from the security incidents happened in healthcare organisations [43]. They collect the security incidents for the same purpose on sharing and exchanging the

lessons learned. However, they have not provided a mechanism to feed back lessons to improve the ISMS.

2.5.2 Lessons learned sharing through incident dissemination

2.5.2.1 Traditional lessons learned dissemination methods

Incident dissemination is enacted through a series of formal reports, informal meetings, emails, newsletters, and presentations to management [3, 36]. Meetings are held and communicative notes are gathered to address responses, disagreements, suggestions and additions to security policies and the incident procedures [3]. Issues to document include an estimation of the damage caused, actions taken during the incident, policies and procedures that require an update and any electronic evidence that can be used for pursuing those responsible [2]. Comparing to the formal incident report, emails, newsletters, meetings and presentations to management contain less information than the post-incident report. They are usually presented in a free-style way and less information are provided to communicate the lessons learned to inform improvements of the ISMS.

There is usually a formal post-incident report produced after the security incident to document findings throughout the incident response process. Information contained in the report is typically classified into business impact and remediation information [3]. Business impact information involves how the incident is affecting the organisation in terms of mission impact, financial impact, etc. For example, “The missing external hard drive is believed to contain numerous research-related files containing personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS), on over 1.3 million medical providers” [15]. Remediation information mainly refers to the suggested actions, plans, procedures, and lessons learned that can mitigate the incidents [3]. For example, “We recommend that the Assistant Secretary for Information and Technology revise VA Directive 6601 to require the use of encryption, or an otherwise effective tool, to properly protect personally identifiable information and other sensitive data stored on removable storage devices when used within VA” [15].

Many organisations do not want to share business impact information with outside companies unless there is clear value proposition or formal reporting requirements. When sharing information with peer and partner organisations, incident response teams

should focus on exchanging remediation information [3]. The remediation information describes (1) the security issues, e.g. “The position sensitivity level for the IT Specialist was inaccurately designated as moderate risk, which was inconsistent with his programmer privileges and resulted in a less extensive background investigation” [15]; (2) the security requirements violated during this process, e.g. “Position Sensitivity Level Assessments were Not Adequately Performed” [15]; and (3) the recommendations, e.g. “We recommend that the Under Secretary for Health direct the Medical Center Director to re-evaluate and correct position sensitivity levels and associated background investigations for positions at the Birmingham VAMC” [15]. This information is inter-related, however, it is scattered throughout a report (Appendix A.5). This issue has been compounded in lengthy security incident reports [15]. Stakeholders responsible for protecting patient data lack the time and the motivation to spend the many hours needed to read and digest existing reports [45]. This creates significant problems within the wider scope of security management systems. It can be difficult to accurately assess the likelihood or consequences of future attacks when managers are unaware of previous incidents.

2.5.2.2 Lessons learned dissemination methods using diagrams

Traditional ways to disseminate lessons learned are based on textual description. The linear format of a text can discourage readers from obtaining comprehensive understanding of relationships among ideas across paragraphs due to working memory limitations [129]. Graphical diagrams can serve this purpose, as it can communicate not only individual elements of information but also relationships among those elements. As Larkin and Simon explained in “Why a Diagram is (Sometimes) Worth Ten Thousand Words”, diagram can be superior to a verbal description for solving problems for three reasons [130],

- Diagrams can group together all relevant information, avoiding large amounts of searching for the elements needed to make an inference.
- Diagrams use location to group information about a single element, avoiding the need to match symbolic labels.
- Diagrams automatically support large scale perceptual inferences, making it extremely easy for humans to do.

He continues to explain that, a diagram must be constructed to take advantage of the above mentioned features. Failing to use these features is probably part of the reason why some diagrams are ineffective to help readers [131].

The diagramming approach has been well studied since then. Purchase has conducted comprehensive review on diagramming approaches and has classified them into abstract and concrete diagrams [132]. Concrete diagram are iconic diagrams that have a perceptual relationship to the objects that they represent, such as the heart and blood circulation [133], seating arrangements [134] and images [135]. Abstract diagrams are symbolic notations, which produce diagrams that have no perceptual relationship to the concepts that they represent. Examples are trees [136], Venn diagrams [137], Unified Modelling Language [138] and Goal Structuring Notations [7].

Empirical case studies [6, 45] have identified the difficulties when text was the only medium available for communicating security lessons. Similar difficulties were identified in safety area, when text was the only approach for expressing complex safety arguments [139]. The free-style text is considered to be unclear and not well structured, the meaning of the text, and therefore the structure of the safety argument, can be ambiguous and unclear [7]. The use of free text makes is difficult to ensure that all stakeholders share the same understanding of the argument [7]. The diagramming approach GSN has been proposed in safety area to address this issue. In particular, it links the evidence to show that particular requirements have been supported. GSN has been found to improve the comprehension of safety arguments and allows lightweight development of an argument [140]. The notation helps to focus the selection of evidence upon satisfying the overall requirements of the systems or applications. GSN has become the dominant approach in the UK defence sector [10], increasingly being used in safety-critical industries to improve the structure, rigor, and clarity of design requirements [7, 47, 48]. The same approach has more recently been extended to document security requirements [45, 49–52]. We believe this approach can be adapted to effectively communicate security lessons into the ISMS. Chapter 3 further expands the work on the theoretical basis of the GSN and the rationale to apply this approach.

2.5.3 Lessons learned sharing in healthcare organisations

In Europe and North America, there are legislative requirements to report security incidents. In the US, the security incidents are reported to Nation's Healthcare and Public Health Information Sharing and Analysis Centre (NH-ISAC) [43]. In the UK, the

NHS must report Serious Untoward Incidents that involve the unauthorised disclosure of confidential patient information to the Caldicott Guardian [141], the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner for consideration of any actions [142]. A Serious Untoward Incident related to Personal Identifiable Data is defined as: “The actual or potential loss of personal data and/or any information that could lead to identity fraud or have other significant impact on individuals or the organisation”. The key aim of serious incident reporting is to reduce the recurrence both where the original incident occurred and elsewhere [142].

In China, there have not been legislative requirements found for healthcare organisation to report security incidents and learn from lessons. Health information security has not attracted significant attention by the healthcare providers and governments [143, 144], although some attempts has been made to protect health information [73, 145–147]. Gao suggests two main reasons for the lack of motivations: (1) the Chinese traditional culture does not address the importance of personal privacy; and (2) healthcare systems in China are still in their infancy and there has not been large-scale health data exchange that can potentially trigger large amounts of serious privacy violations [148]. However, the implementation of healthcare information systems can hardly be successful if health information privacy cannot be ensured [149]. There is a need for China to learn successful practices from international experience to improve their healthcare information security management systems [148].

2.6 Context of the research

Based on the literature review and discussion of this chapter, we have identified the theoretical and industrial motivations of this research:

- Information Security Management System (ISMS) frameworks such as FIS-CAM, ISO 27001, and GB/T22239 can be used as a basis for developing security procedures and good practices within an organisation. However, these frameworks have been criticised, as based on personal observations and common practices. Improvements of those frameworks can benefit from lessons learned on how the objectives of security standards are met in organisations where information security management standards are applied. Lessons learned from the security incidents can be used to improve procedures, policies, risk assessment and controls [5]. However, the key learning points are not effectively fed into

security processes, management structure, policies, procedures and risk assessment [6]. There is a need to translate the learning from security incidents to inform improvements of the ISMS.

- Incident response is an important part of ISMS [34]. However, current literatures show that incident response is typically limited to the technical process and does not leverage opportunities to learn about the security lessons [37, 38]. The incident response has focused on solving the direct cause of the incident, rather than investigating the in-depth cause which is often not a technical problem (e.g. firewall not properly configured) but a policy problem (e.g. there is not a security requirement on the configuration of the firewall). This imbalanced focus has resulted in the loss of opportunities to investigate why a potential incident is not adequately covered by the policy, that may lead to further improvements of policy and may prevent future incidents which may not directly relate to this incident.
- There are government programs and legislative initiatives pressing organisations to report security incidents, which allows lessons learned to be shared and to prevent the re-occurrence of security incidents. This has indicated the importance to share and exchange the lessons learned. Although it has not provided a mechanism to feed back lessons to improve the information security management systems. It fosters an environment where different stakeholders speak the same language, when exchanging lessons learned from security incidents.
- Incident dissemination relies on formal reports, emails, newsletters, meetings and presentations to management [3, 36]. Post-incident reports contain more detailed information compared to the other means. A post-incident report is a formal report generated to document information obtained during the security incident investigation. It contains comprehensive information typically classified into business impact and remediation information. When sharing information with peer and partner organisations, incident response teams should focus on exchanging remediation information [3]. These include the violated security requirements, the security issues and their corresponding recommendations as well as their inter-related relationships. However, this information is usually scattered in the lengthy textual report, which can be hundred of pages. There is a need of a method to bring together this information in a way that can be easily understood and shared among people who need it.

- Communicating security lessons is difficult when text was the only medium available. Graphical diagrams can be adopted to address this problem, as it can communicate not only individual elements of information but also relationships among those elements of information. The diagramming approach GSN has been proposed in safety area to address similar issues. In particular, it links the evidence to show that particular requirements have been supported. We believe this approach has the potential to address our research problem and can be adapted to effectively communicating security lessons into ISMS.
- Symantec has reported an increase of security incidents in healthcare [17]. These incidents can have negative effects on an organisation's reputation and individual's confidence towards this organisation [26]. Healthcare organisations are under increasing pressure from the legislative initiatives and obliged to report the security incidents so as to improve information security management. Therefore, it is imperative for the healthcare organisations to learn the lessons from those security incidents to inform improvements of the ISMS.

Based on the analysis above, there is a need to propose a systematic method to synthesis the lessons learned collected from the security incidents, and translate them in a way that can be easily communicated with the ISMS. In particular, the diagramming approach, Goal Structuring Notations, will be adapted to communicate security lessons with the ISMS. The next chapter elaborates on the proposed approach.

Chapter 3

The Generic Security Template

In Chapter 2, we have identified the theoretical context of this research. This chapter introduces a novel approach, the Generic Security Template, to feed back the lessons learned from security incidents to the ISMS. We have chosen to base our work on an existing approach, the Goal Structuring Notations (GSN). The host of public resources describing how to apply this approach can help to reduce the costs of training staff. The novelty of our approach lies instead in the use of GSN to construct Generic Security Template that links aspects of a previous security breach to the more generic standards, policies, procedures and technical innovations that are intended to avoid any recurrence of an adverse event.

This chapter is divided into the following sections. Section 3.1 introduces the basis of the Generic Security Template, including the concept of argumentation and assurance case. Section 3.2 introduces the graphical notation, Goal Structuring Notations (GSN) that we adopt to create the Generic Security Template. Section 3.3 defines the Generic Security Template and outlines the processes on how to apply the Generic Security Template to derive insights from security incidents. Section 3.4 presents the Generic Security Template Pattern. Section 3.5 discusses about the evaluation aspects of the Generic Security Template. Section 3.6 summarises this chapter.

3.1 Assurance cases

3.1.1 Arguments and assurance cases

An argument is “a reason or set of reasons given in support of an idea, action or theory” [150]. An argument can be defined as a set of premise claims put forward for support-

ing another claim, the conclusion. A premise is a supporting reason in an argument. A conclusion is the claim that the premises are intended to support. In an argument, evidence is provided to convince others that their claim is true. An argument defines the relations that link evidence, premise claims with its supported claim, and can be used for justifying how the sub-claims and evidences are organised together to support a conclusion [151].

The concept of the assurance case has been derived from argument theory [151, 152]. It is defined as “a documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system’s properties are adequately justified for a given application in a given environment” [152].

Assurance cases have been widely used within the safety area. A safety assurance case is defined as “a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment” [153]. Safety assurance case has been widely used in nuclear and defence industries as well as rail and civil aviation [11], and is now a requirement of UK Ministry of Defence Standard 00-56 [154]. Safety assurance case has been recently introduced into healthcare as people start realising the misuse of health IT system can deviate its intended operation and pose a risk to the patients. The use of the safety cases aims to reduce risks or uncertainty of the risk to operate a health IT system [155].

A security assurance case could be defined as “a documented body of evidence that provides a convincing and valid argument that a system is adequately secure for a given application in a given environment”. ISO 15026 introduces the concept of a security assurance case [156]. This has generalized the use of assurance cases beyond the safety area. John Goodenough, Howard Lipson, and Chuck Weinstock present a security assurance case. They claimed system security through addressing potential deficiencies arising at different stages of the software development life cycle [157]. Vivas integrates assurance case creation with system development on mobile communities and community-supporting services, with special emphasis on privacy, trust, and identity management [158]. However, security assurance cases have not been widely used in system security management [159]. Although researchers have demonstrated the practical benefits in performing a combined analysis and documenting a combined argument for both safety and security [160], the industry adopted safety arguments more broadly than security arguments.

Conformance argument [161] has extended the work of assurance cases, and has been applied to evaluate software assurance standards [162]. It can be defined as “a

structured, comprehensive, and defensible argument demonstrating that the evidence is sufficient to show that an artefact adequately meets the standard's requirements". Instead of arguing how evidence supports a system requirement in system safety, a conformance argument justifies belief in conformance. According to the definition of conformance argument, the first level of decomposition is over the standard's requirements. Claims are further decomposed until each sub-claim can be supported by evidence. It illustrates the developers' interpretation of the standard and defines what evidence must be provided to demonstrate a specific system conforms to a given standard.

The Generic Security Template proposed in this thesis builds on existing work into security assurance. Instead of collecting evidence to argue that the design and operation of an existing application are acceptably secure, we have developed the Generic Security Template to collect the insights that have been derived when a system has proven NOT to be acceptably secure. We use the same syntactic components of the GSN to document the lessons learned (i.e. information about the causes of a breach and subsequent recommendations) from security incidents. Our initial work focuses on developing the approach to support the security requirements of healthcare information security management systems. This is justified by the large number of data breaches within this area and also by the impact that such disclosures can have on patients and their relatives. More details on the Generic Security Template will be provided in section 3.3.

3.1.2 Graphical notations

Kelly has reviewed several approaches to present safety arguments, including free text, tabular structure, claim structures, Bayesian belief networks [7]. He argues that, *well structured approaches to express safety arguments in text* can be difficult to present complex arguments and ensure that all parties share the same understanding. The single table of the *tabular structure* can only present two steps in the decomposition of the argument (i.e. claim \rightarrow argument and argument \rightarrow evidence). For complex arguments, which may contain many levels of claim and sub-claim, the table will become very complex or involve multi-tables, then the clarity or the flow of the argument will be lost. The *claim structures* are built from a number of claims joint together by AND and OR gates. It represents the cut down version of the GSN, which has no means of expressing argument strategies. They do not graphically communicate rationale,

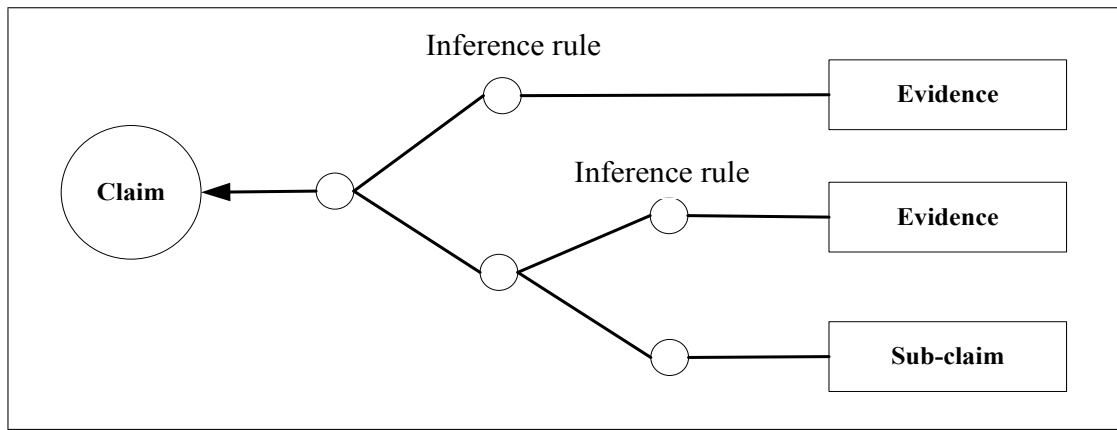


Figure 3.1: CAE argument structure [10]

context or the role of evidence. The *traceability matrices* indicate a relationship between statements. However, they can only present one layer at a time and provide no means to justify the relationships between statements of different levels. *Bayesian belief networks* [163] are graphical networks that communicate the probability causal relationships between variables. However, the determination of the conditional probabilities can be a hugely subjective exercise [7].

Other work includes Holloway's five styles of text-based representations for safety arguments [164]. It reports the same problems of textual based approaches. The resulting text-based safety/security cases are usually cumbersome, or difficult to review due to the massive relations between safety/security considerations. The logic of the argument itself is often lost in large volumes of paper document.

Claims-Argument-Evidence (CAE) [10] is introduced by Bloomfield in 1998. According to Bloomfield's definition, a *claim* is about a property of the system or subsystem; *evidence* is used as the basis of the argument, which can be facts, assumptions, or sub-claims, derived from a lower-level sub-argument; *argument* is used for linking the evidence to the claim, which can be deterministic, probabilistic or qualitative; *inference* is the mechanism that provides the transformational rules for the argument [153]. The CAE argument structure is shown in Figure 3.1.

The Goal Structuring Notation (GSN) was developed in the early 1990s and has undergone significant development and refinement since then. Compared to CAE, GSN has a richer range of symbols in expressing arguments. GSN is the dominant approach in the UK defence sector. It is used in safety-critical industries to improve the structure, rigor, and clarity of safety arguments. Within Europe, GSN has been adopted by a growing number of companies within safety-critical industries (such as

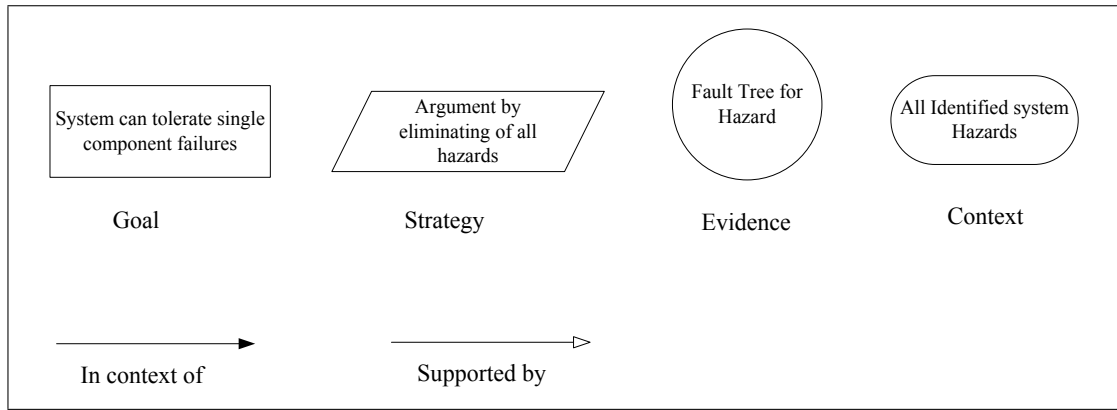


Figure 3.2: GSN Notations [11]

aerospace, railways and defence) for the presentation of safety arguments within safety cases [11]. Moreover, GSN has been included in the software assurance standard ISO 15026 [156]. Given the broad acceptance of GSN, we adopted this approach in this dissertation.

3.2 Goal structuring notations (GSN)

GSN can be used to present argument by creating a graphical structure between goals, sub-goals, evidence/solutions, strategies and contexts [11]. GSN has been found to improve the comprehension of safety arguments and allows lightweight development of an argument [140]. The notation helps to focus the selection of evidence upon satisfying the overall objectives (or requirements) of the systems or applications.

3.2.1 GSN elements and notations

Figure 3.2 presents the core symbols used in GSN: *Goal*, *Strategy*, *Solution/Evidence* and *Context*, as well as *Supported by* and *In context of*. A *Goal* is a claim, the statements that the goal structure is designed to support. *Evidence* exists to support the truth of the claimed goal, which can be documented by providing a solution in GSN. *Strategy* is inserted between goals at two levels of abstraction, to explain how the top-level goal is addressed by the aggregation of the goals presented at the lower level. *Context* is used to declare supplementary information and provide adequate understanding of the context surrounding the claim/strategy. Usually it presents concept clarification introduced in the claim/strategy [11].

3.2.2 Goal decomposition methods

3.2.2.1 Developing goal structures top-down

A top down approach to goal development starts with top goal identification, followed by context identification providing the basis on which the goals are stated. The strategies are then identified for providing reasons why the claimed goal is true. Contextual information of the strategy is also required to understand the argument approach. The goal structure continues to be developed in this way until it is clear that no further decomposition is needed and the goal can be directly supported by evidence artefacts (e.g. test results). Below are the steps of a top down approach to goal development [11],

Step 1: Identify the goals to be supported (Identify the top goal(s) of the structure).

Step 2: Define the basis on which the goals are stated (Identify the context of the goal).

Step 3: Identify the strategy used to support the goals (Substantiate the goal). What reasons are there for saying that the goal is true? What statements would convince the reader that the goal is true?

Step 4: Define the basis on which the strategy is stated. Identify the contextual information required to understand the argument approach.

Step 5: Elaborate the strategy (Elaborating a strategy involves defining new goals). The goal structure continues to be developed in this way until it is clear that no further decomposition into sub-goals is necessary and the goal can be directly supported by appeal to some evidence artefact.

Step 6: Identify the basic solution/evidence.

3.2.2.2 Developing goal structures bottom-up

The following process can be used to develop a goal structure bottom-up [11],

Step 1: Identify evidence to present as solutions.

Step 2: Infer “evidence assertion” goals to be directly supported by these solutions.

Step 3: Derive higher-level sub-goals that are supported by the evidence assertions.

Step 4: Describe how each layer of sub-goals to satisfy their parent goal i.e. strategy.

Step 5: Check that any necessary contextual information is included.

Step 6: Check back down the structure for completeness.

Step 7: Join the resulting goal structure to known top goal or set of sub-goals.

The bottom-up approach is rarely used in isolation to form a complete goal structure. It usually joins to a desired higher-level goal that is already understood to be a requirement of an assurance case [11].

3.2.3 Safety arguments and the GSN

Safety arguments are typically communicated in safety cases through free text and the GSN [7]. Kelly cited the following textual descriptions from a real industrial safety case to explain the problems experienced when text is the only medium available for expressing complex arguments.

“For hazards associated with warnings, the assumptions of Section 3.4 associated with the requirements to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.” [7].

Several communication concerns were identified with this paragraph. The free-style text was found to be unclear and not well structured. The meaning of the text, and the structure of the safety argument, can be ambiguous and unclear. This problem became compounded by the frequently used cross-references in a safety case as an integrator of evidence. Multiple cross-references can disrupt the flow of the main arguments. The use of free text makes it difficult to ensure that all stakeholders share the same understanding of the argument, which resulted in inefficient and ineffective safety case management [7]. Johnson has identified the same difficulty in analysing accident reports. It is difficult to draw particular conclusions from the many hundreds of pages of evidence from those reports, as the logic can easily get lost across the paragraphs of contextual details [139].

Goal Structuring Notation (GSN) clearly represents the individual elements of the safety argument (requirements, claims, evidence and context). An example safety case is provided in Figure 3.3, taken from [11]. In this diagram, the top goal is “C/S (Control System) Logic is fault free”, the statements that the goal structure is designed to support. The structure is broken down into sub-goals, either directly or, as in this case, or indirectly through a strategy. The two argument strategies put forward as a means of addressing the top level goal are “Argument by satisfaction of all C/S (Control System) safety requirements”, and, “Argument by omission of all identified software hazards”.

These strategies are then elaborated by five sub-goals. The goal structure continues to be decomposed this way until it can be supported by evidence. For example, the goal “Unintended Closing of press after PoNR (Point of No Return) can only occur as a result of component failure”, is supported by reference to the solutions, “Fault tree cutsets” and “Hazard Directed Testing Results”.

3.2.4 Security arguments and the GSN

The formal post-incident report and notes collected from incident dissemination methods contains valuable information presenting an informed security argument on how the causes of an incident is addressed by the remedial recommendations. As we have identified in the literature review, they contain valuable information such as (1) the security issues; (2) the security requirements violated during this process; and (3) the recommendations. However, these informal arguments are usually based on lengthy textual descriptions. We aim to apply the GSN to present security arguments on how the issues and their corresponding remedial recommendations are gathered together to address different levels of security requirements violated in the security incidents.

We have conducted several preliminary case studies [45] into the use of GSN with real world security incidents in healthcare organisations in the US and China. The aim was to find out whether GSN can be used to feed back the security lessons to the ISMS. We analysed the security incident reports of the Veterans Affairs data leakage incident happened in 2006 [14] and 2007 [15] in the US. The security lessons were written using free text in documents, which are over 100 pages. We were able to identify the security lessons and map them to the higher-level security requirements that are defined in FISCAM. We also analysed a news clip about an incident happened in the Shenzhen hospital in China. Since there was no official report, we were forced to rely on media sources. We were also able to map the lessons to higher-level security requirements defined in the Chinese security standard, GB/T22239. Those case studies established the feasibility of structuring security lessons using GSN.

3.3 The Generic Security Template

Within safety area, generic safety arguments were developed to facilitate the initiation and development of safety arguments. There are generic safety arguments developed for IMA-based avionic systems [47], and the generic goal-based safety case for justi-

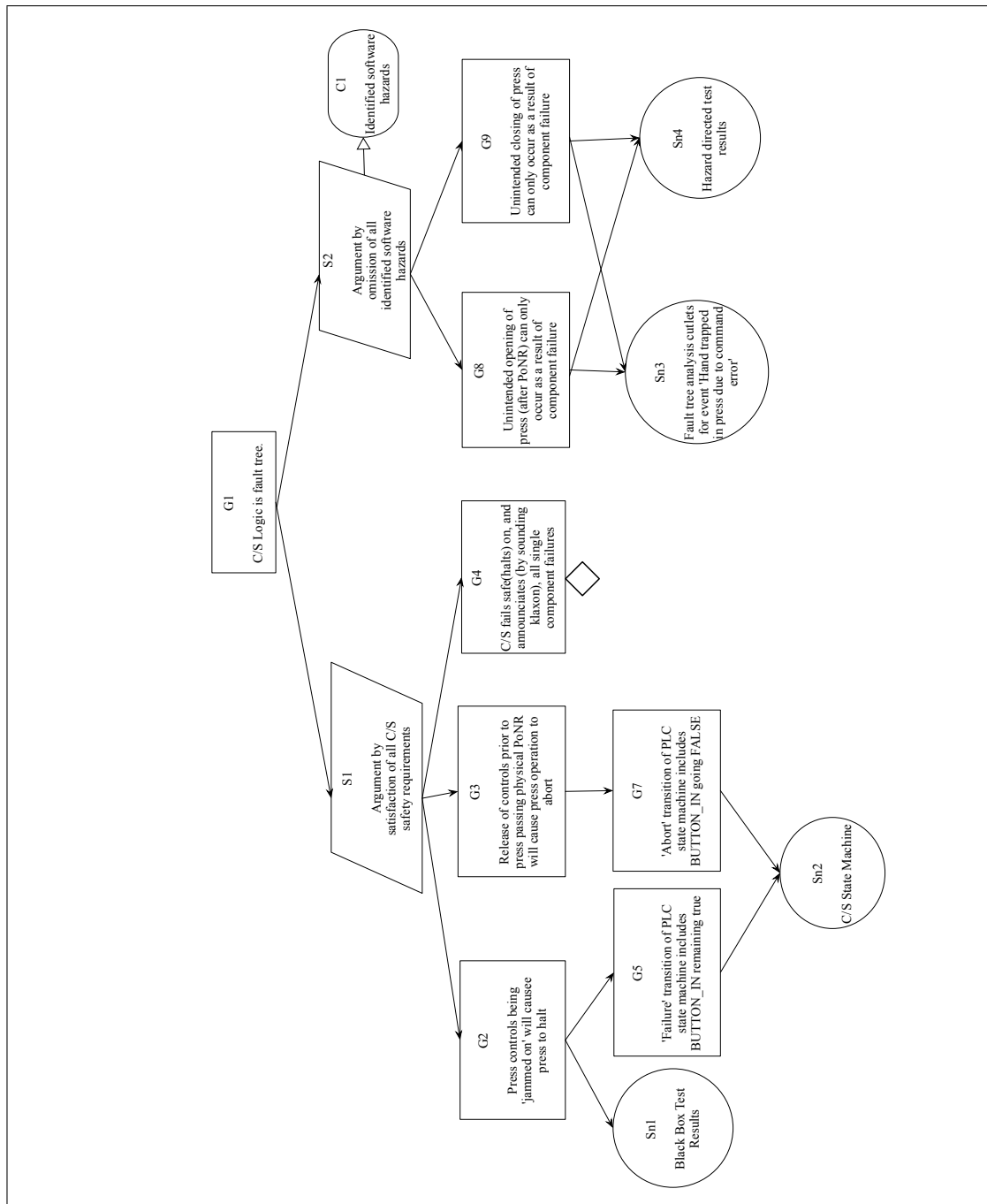


Figure 3.3: An example instance of the Safety Case [11]

cation and presentation of formal analysis to the certification authorities [48]. Within security areas, less research work can be found in generic security arguments. Based on the preliminary case studies into the use of GSN with real world security incidents in healthcare organisations in the US and China [45], this section defines the Generic Security Template and outlines the steps on how to apply the Generic Security Template to derive insights from security incidents.

3.3.1 Definition of the Generic Security Template

We define a Generic Security Template as “*a documented body of lessons learned identified from a security incident that can support the Security Requirements of the Information Security Management System (ISMS)*”. A *security incident*, is defined as “a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices” [53]. *Lessons learned*, are defined as the knowledge or understanding gained by experience [54]. In this dissertation, it refers to (1) security issues (the causes of a security incident in confidentiality); and (2) security recommendations (intended to avoid any recurrence). *Security Requirements of the (ISMS)*, is presented in the form of a specific security standard or guideline applied to the organisation where the security incident happened. The Generic Security Template links the analysis of an incident to specific security standards or guidelines that help to implement particular recommendations. *Generic*, is defined as “characteristic of or relating to a class or group of things; not specific” [165]. In this thesis, Generic Security Templates are intended to be applicable across different classes of organisation and not specifically to the place where an incident occurred.

Based on the definition, the principle GSN notations are customised as is shown in Figure 3.4, the *Evidence/Solution* notation is replaced by *Lessons learned*. Within the *Lessons learned*, for example, “Position Description” is the security issue, and the recommendation is “Re-evaluate and correct position sensitivity levels”. We have decided to alter the *Evidence/Solution* notation rather than adding a new one because those lessons learned have been implemented by the organisation and can serve as solutions to support security requirements, hence to formulate a security argument. The strategies used to support these recommendations include reference to the policies, standards and guidelines that are intended to prevent any recurrence of an incident. In some cases, the recommendations in an incident may include changes to the guidance within a particular industry or organisation. In such instances, the Generic Security

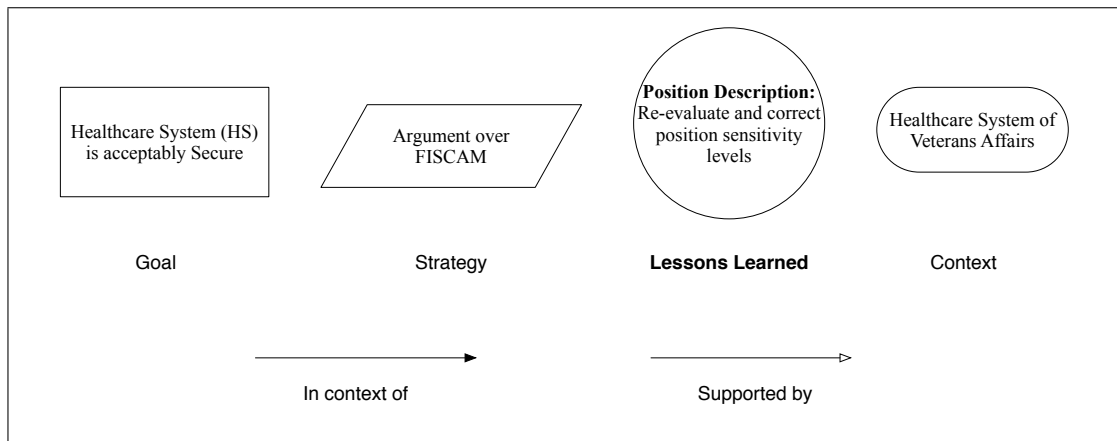


Figure 3.4: Customised GSN Notations

Template will link the finding to a revised version of the security documentation so that end users can identify the new procedures that are intended to prevent future breaches.

The Generic Security Template is a theoretical model that maps the lessons learned obtained from the security incident to the security standard or guideline in a structured manner. The Generic Security Template that describes a specific security incident is defined as a GST instance. Figure 3.5 is an example instance of the Generic Security Template (See Chapter 4 Section 4.2) created for Veterans Affairs Data Leakage Incident 2007 [15] happened in United States. The steps to create an instance of the Generic Security Template are provided in the following sections.

3.3.2 The Generic Security Template and assurance cases

The Generic Security Template builds on existing work into security assurance. Instead of collecting evidence to argue safety, it collects the security recommendations to support different levels of security requirements of an information security management system. The Generic Security Template will turn into an assurance case, if there is evidence showing that those recommendations have been fulfilled. However, it is organisation's responsibility to decide whether they have accepted and fulfilled those recommendations.

3.3.3 Creation of instances of the Generic Security Template

A GST instance provides a graphical overview of the mapping between the causes/recommendations derived from security incidents and the guidelines/policies/standards that are intended to prevent any recurrence of a data breach. We use the US Veterans

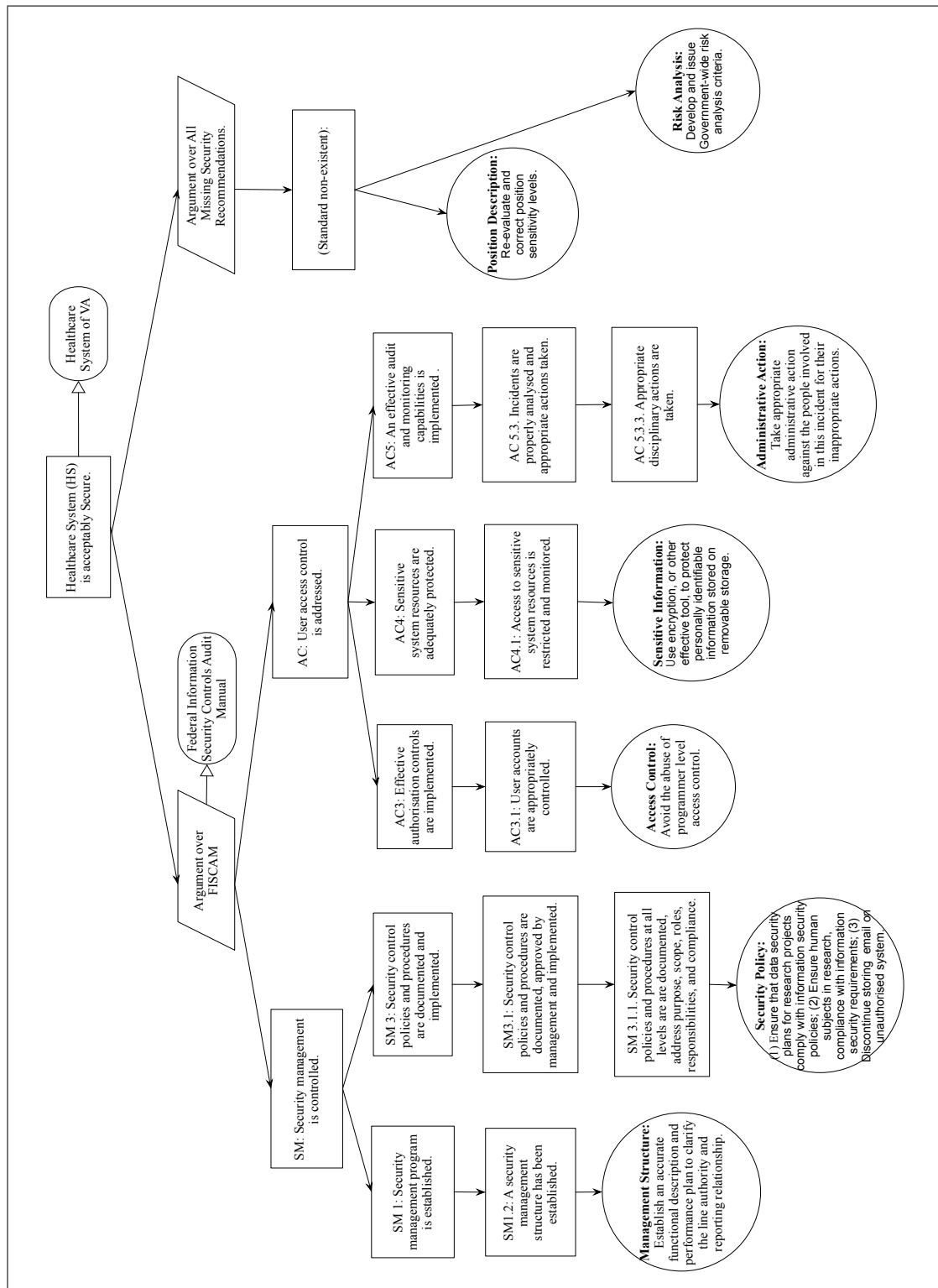


Figure 3.5: An example instance of the GST - VA 2007 Data Leakage Incident

Affairs (VA) Data Leakage Incident 2007 to illustrate the creation steps. Figure 3.5 presents the diagram created for this real world case study. As is mentioned, it is based on a report into the disclosure of personal information about veterans and over medical providers by the US Veterans Affairs Administration (VA) [15]. Below are the four steps to create a GST instance.

3.3.3.1 Step 1: Prepare the goal structure

The top level goal is to ensure that a healthcare system is acceptably secure. We used the word "acceptably" as absolute security is unachievable. Within the GST, the security argument is there to convince someone that the system is secure enough when compared against a specific security standard applied by the organisation. This high-level goal is then decomposed into sub-goals that each reflects more detailed security requirements within a security management system. The goal structure decomposition continues in this way until it reaches the level that can be directly supported by appealing to the recommendations identified in an incident report.

In our approach, we have simplified the process of identifying sub-goals by using security requirements within the applicable standards and guidelines in particular healthcare organisations. This helps to increase the genericity of our approach. The goal structured is pre-created to help the users get started. For example, in the case study of the VA 2007 Data Leakage Incident, we have used security requirements of the general controls (i.e. security management, access controls, configuration management, segregation of duties and contingency planning) in Federal Information Security Control Audit Manual (FISCAM). As is introduced in Chapter 2, FISCAM includes general controls categories such as security management, access controls, configuration management, segregation of duties and contingency planning. For each of those general control areas, it identifies several critical elements that are essential security requirements for establishing adequate security controls.

In this step, we borrowed the experience of conformance argument in safety area, where the goal structure has been used to represent safety standards. Instead of arguing how evidence supports a system requirement in system safety, a conformance argument justifies belief in conformance. The decomposition of sub-goals is over the safety standard's requirements.

3.3.3.2 Step 2: Identify the lessons learned from the security incident

Lessons learned are identified by searching incident reports for security issues and recommendations. A review of the existing incident reports [14–16, 44] show that the security analysts are able to describe learning points using structured text. However, there has not been a unified definition on an appropriate level of details that a lesson learned should contain. The security analysts define their own level of details in the security incident report according to individual business needs. However, too much information will undermine the effectiveness of the graphical presentation, while too little information will make it difficult to understand. In this step, the analyst has to identify key learning points. These are then introduced into the Generic Security Template using a structured textual format. For the security issue, we recommend to use short <Noun-Phrase>, for example, “Sensitive Information”, as a short description of a specific security issue. For the recommendation, we recommend the statement to be in the form of <Verb-Phrase> <Noun-Phrase>. For example, “Use encryption or effective tool to protect personally identifiable information”. This is different from Kelly’s work in using the <Noun-Phrase> as evidence/solution such as “test result” to support the truth of the goals. The security issue and its corresponding recommendation will become the *Lessons learned* part of the Generic Security Template.

3.3.3.3 Step 3: Map the Lessons learned to the Goal Structure

The lessons identified in Step 2, typically contain different levels of details, can be mapped to different levels of the goal structure. This has achieved by using the bottom up approach and the analyst has to identify the relationships between security sub-goals, based on standards, guidelines and policies, and the lessons learned from a previous security incident. For example, as is shown in Figure 3.5, the lessons learned “Access Control: Avoid the abuse of programmer level access control”, was found to be related and mapped to the goal “AC 3.1 User accounts are appropriately controlled”.

There are the cases when the lessons learned could not find a goal to map to. For example, as is shown in Figure 3.5, the lessons learned “Position Description: Re-evaluate and correct position sensitivity levels” and “Risk Analysis: Develop and issue Government-wide risk analysis criteria”, could not find goals to map to. These lessons learned are mapped to a newly created goal named “Standard non-existent” and directly link to the top goal. This probably because the existing goals, based on standards, guidelines or policies have missing requirements that are not covered those

learning points. This may also due to the unsuitability to add those lessons into security standards, guidelines or policies. For example, some recommendations may refer to the process for managing a system, or the meta process of reporting incidents across organisations. However, these newly identified lessons need further assessment in terms of whether they are suitable to be included in the existing security standards/guidelines.

A key benefit of our approach is that their subjective reasoning is documented in the nodes of the Generic Security Template. A range of stakeholders can then check the resulting diagrams to determine when key lessons have been omitted or if additional work is required to support the exchange of security lessons. They could check the reasoning and experience can be borrowed from safety area on how to avoid and detecting fallacious reasoning in the arguments [166]. The use of a graphical notation provides stakeholders with an overview of key issues before being forced to read the hundreds of pages of detailed prose that increasingly documents the findings of security investigations.

3.3.3.4 Step 4: Elaborate the Context and Strategy

Strategies are inserted between goals and sub-goals; they justify goal decomposition. They typically refer to the goal decomposition methods, such as the use of security standards, organisational guidelines or technical documentation. As before, we have exploited a simplified sentence structure that is intended to improve the clarity of the diagram as used in the safety arguments [7]; “argument by <approach>”, “argument over <approach>”, “argument using <approach>”, “argument of <approach>”. For example, “Argument over FISCAM”.

Recall step 3, there are some lessons learned that are not covered by the existing goal structure, they are mapped to a newly create goal named “Standard non-existent”. A new strategy named “Argument over all Missing Security Requirements” is created and inserted between the top goal and the goal “standard-do-not-exist” to present such argument.

The context notations need to be elaborated during this process by providing supplementary information for a specific incident such as in Figure 3.5, “Federal Information Security Controls Audit Manual”, this context information is used to explain the concept “FISCAM” in the strategy.

3.3.4 Pre-requisites to apply the Generic Security Template

The target users of the Generic Security Template will be the people responsible for protecting customers' personal private information within an organisation. For example, in healthcare organisations, both healthcare professionals and IT professionals have the responsibility to protect patients' private information. However, the application of the Generic Security Template resides on the expertise of the organisation's incident handling capacity. Organisations have to satisfy the following pre-requisites to apply the Generic Security Template,

- *Expertise of information security.* The organisation should have an incident handling team [35, 53] consists of security analysts with incident handling expertise. They should be able to analyse an incident and justify actions taken to address an incident.
- *Incident reporting with useful recommendations.* The organisation should have incident reporting [35, 167] mechanism allowing for useful security lesson learned in different forms (e.g. technical notes, security incident reports, etc.) generated from the incident handling process.
- *Security requirements elicitation.* The organisation should have security requirements elicited [100] based on existing security standards, guidelines or procedures.

3.4 The Generic Security Template Pattern

3.4.1 GSN Pattern

It is important to recognise that our development of Generic Security Templates is, in part, motivated by previous work into design patterns. Alexander [159] describes how patterns “describe a problem which occurs over and over again in our environment, and then describes the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice”. The field of design patterns has become well established since the publication of the book “Design Patterns - Elements of Reusable Object-Oriented Software” [168] by Gamma, Helm, Johnson and Vlissides (the “Gang of Four”). Kelly adapted the concept of patterns to GSN safety arguments “A means of documenting and reusing successful safety

argument structures” [7]. An interview study with 29 interviews including developers, consultants, managers, and assessors shows that patterns provide a good starting point for safety argument construction and has estimated that the long-term benefits of pattern-based safety case development more than outweigh the (initial) costs [169]. Table 3.1 lists the symbols used to support the pattern design, which is an extension of GSN. Those are the Multiplicity Extensions and Entity Abstractions [7]. Explanation of the symbols are provided in Table 3.1.

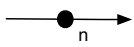
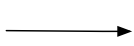

Type	Notations	Notation Description
Multiplicity Extensions		A solid ball is the symbol for many (meaning zero or more). The label next to the ball indicates the cardinality of the relationship
		A line without multiplicity symbols indicates a one to one relationship (as in conventional GSN)
Entity Abstractions		Uninstantiated Entity. This placeholder denotes that the attached entity remains to be instantiated i.e. at some later stage the ‘abstract’ entity needs to be replaced (instantiated) with a more concrete instance.

Table 3.1: Extension of GSN Pattern Design Notations [7]

3.4.2 The Generic Security Template Pattern

Based on the steps in section 3.3.3, the Generic Security Template Pattern is created as shown in Figure 3.6. Whereas Figure 3.5 presents an instance of a Generic Security Template, Figure 3.6 provides a more generic overview which abstracts away from the specifics of the VA case study to provide the general structure of our analysis. It is not intended that this diagram will be visible to the end users of an incident report but that it provides a template for the security professionals and risk managers who coordinate the creation of a specific security template after each incident.

Within the pattern, G1 is the top level goal claiming that “System X is secure” within the context of C1 “ISMS for System X”. It is then divided into sub-level goals using the strategies that “argument over Security Standard X” and that “argument over Missing Requirements”. Within Strategy S1, the concept “Security Standard” is explained in C2 “Security Standard for System X”. Under Strategy S1, we have used the structured security requirements in the Security Standard as the goal structure; G3 ... GN represent different level (1 ~ n) of goals (security requirements) in the goal structure (security standards/guidelines). LL1 are the lessons learned deemed to be related to a specific goal (security requirement). Under Strategy S2, the Missing Requirement

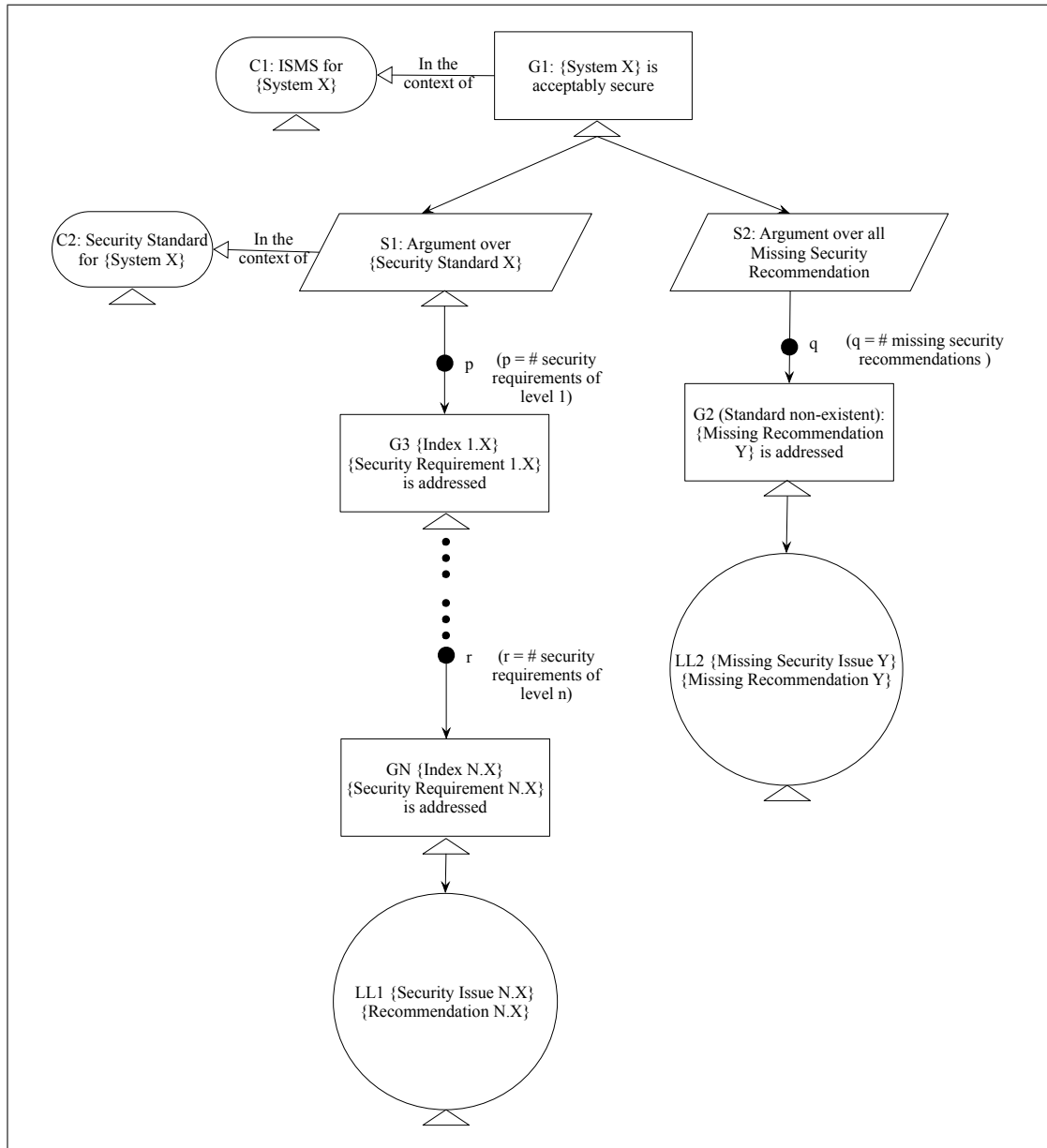


Figure 3.6: The Generic Security Template Pattern

Y are identified and included in the goal structure. G2 represents a new goal (security requirement) created for the Missing Requirement Y. LL2 are the lessons learned deemed to be related to none of the goals (security requirements) in the goal structure (security standards/guidelines). A new goal is created for LL2 and link to the top goal through Strategy S2.

This is an abstract description of the Generic Security Template, which can be refined by adding more information about a specific incident. Security professionals must instantiate the values associated with particular incidents to map the lessons learned from a particular report into graphical overviews such as that shown for the VA case study in in Figure 3.5. A detailed guidance on how to instantiate this pattern can be found in section 3.3.3.

3.5 Evaluation of the Generic Security Template

We have proposed a new approach, the Generic Security Template, to present the lessons learned from the security incidents. It is created using the Graphical Structuring Notations (GSN). In particular, it maps the lessons identified from security incidents to the security requirements of the ISMS. We have identified the following aspects for evaluating this approach,

1. The Generic Security Template provides a new way to present lessons learned from security incidents. The novel aspect is that it maps the lessons with different levels of details to different levels of the security requirements. It also helps identify lessons that the security standards do not consider. However, the suitability of the Generic Security Template needs to be tested by showing that it can present lessons from real world security incidents. In chapter 4, we conduct several case studies from North American, UK and China and produce several instances of the Generic Security Template. Moreover, the Generic Security Template also needs to be tested by others to show that someone else can create an instance of the Generic Security Template. This will be addressed using an empirical study introduced in Chapter 7.
2. The Generic Security Template is a diagramming presentation of security incidents. As is similar to other diagramming approaches, there can be comprehension barriers due to the new way of presentation. It is worthwhile to conduct a

preliminary study on the comprehension of the Generic Security Template before introducing it into industry. Studies in safety area show that safety cases created using GSN can provide a better comprehension compared to text based documents [140]. In this dissertation, we need to determine if people can better identify the lessons learned from the security incidents by using the Generic Security Template than using the traditional text-based method alone. We conduct an empirical study to test this hypothesis in Chapter 5.

3. The Generic Security Template provides a way to feed back the lessons learned to the ISMS and we believe it can be applicable in healthcare industry. However, the decision has to be made by those in healthcare organisations. In Chapter 6, we conduct an industrial evaluation with people who have experience dealing with patient data to find out how this approach can feed back lessons from security incidents to the ISMS and their acceptance of this approach. In Chapter 8, we further investigate how the lessons learned from security incidents can be transferred from one healthcare organisation to another in a very different context.

3.6 Summary

This chapter introduces a new approach, the Generic Security Template, to present the lessons learned from security incidents. The suitability of the Generic Security Template needs to be tested by showing that it can present lessons learned from the real world security incidents. In the next chapter, we conduct security incidents case studies from US, UK and China and produce several instances of the Generic Security Template by following the creation steps outlined in this chapter.

Chapter 4

Instances of the Generic Security Template

Chapter 3 introduced an approach, the Generic Security Template, to present the lessons learned from the security incidents. The suitability of the Generic Security Template needs to be tested by showing that it can present lessons learned from the real world security incidents. In this chapter, we conduct four security incidents case studies from the US, UK and China and produce four instances of the Generic Security Template from those case studies.

This chapter is divided into the following sections. Section 4.1 analyses the Veterans Affairs data leakage incident happened from 2006. Section 4.2 analyses the Veterans Affairs data leakage incident happened in 2007. Section 4.3 analyses Shenzhen pregnant women's data leakage incident from 2008. Section 4.4 analyses the NHS IT asset data leakage incident. Section 4.5 summarises this chapter.

4.1 Veterans Affairs (VA) data leakage incident 2006

4.1.1 Case description

“On Wednesday, May 3, 2006, the home of a VA Information Technology Specialist was burglarized resulting in the theft of a personally-owned laptop computer and an external hard drive, which was reported to contain personal information on approximately 26 million veterans and United States military personnel. The employee immediately notified Office of Policy, Planning, and Preparedness (OPP&P) management. He also notified the VA Office of Security and Law Enforcement, which is part of the

OPP&P organisation. The employee advised all of them that the stolen personal computer equipment contained VA databases and other files containing veterans' personal identifiers such as name, social security number, military service number, claim number, date of birth, addresses and so on. On June 28, 2006, the stolen laptop computer and external hard drive were recovered intact. Based on all the facts gathered thus far during the investigation, as well as the results of computer forensics examinations, the FBI and OIG are highly confident that the files on the external hard drive were not compromised after the burglary.” [14]

4.1.2 Instance of the Generic Security Template

Step 1: Prepare the goal structure.

We have used the structured category of security requirements in FISCAM, specifically the general control section, as the goal structure for this security incident. FISCAM provides best practices on security control techniques and audit procedures. General controls are designed to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. It includes security management, access controls, configuration management, segregation of duties and contingency planning. For each of these general control areas, it identifies several critical elements and best practices that are essential for establishing adequate controls. These form the goal structure for the VA 2006 data leakage incident.

Step 2: Identify the lessons learned.

Lessons are identified by searching incident reports for security issues and recommendations. The analyst needs to identify key learning points. These are then introduced into the Generic Security Template using a structured textual format. For the security issue, we recommended to use short <Noun-Phrase>, for example, “Sensitive Information”, as a short description of the security issue. For the recommendation, we recommended the statement to be in the form of <Verb-Phrase> <Noun-Phrase>. For example, “Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage”. The identification of the rest of the security issues and recommendations follows the same approach and can be found in Table 4.1,

Table 4.1: Veterans Affairs (VA) data leakage incident 2006

Security Issues	Security Recommendations
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage
Position Description	Define the position sensitive level.
Security Training	Provide linkage to all applicable laws and VA policy as part of the security awareness training.
Incident Handling	Enhance incident-response program for promptly identification and thoroughly investigation of the incidents.
Administrative Action	Take appropriate administrative action against the people involved in this incident for their inappropriate actions.

Step 3: Map the lessons learned to the goal structure.

The lessons identified from the security incident are mapped to the goal structure prepared in Step 1. In this case, those lessons are mapped to the security requirements in FISCAM. As is mentioned in section 3.3.3, the lessons contain different levels of details and can be mapped to different levels of the goal structure. The analyst has to identify the relationship between security sub-goals, based on standards, guidelines and policies, and the lessons learned from a previous security incident. For example, the lesson learned “Incident Handling: Enhance incident-response program on promptly identification and thoroughly investigation of the incidents” is found to be exclusively related to bottom level goal “AC 5.1.1 An effective incident-response program has been implemented”. Therefore, the lesson learned should be mapped to this related goal. The rest of lessons learned are all found to be exclusively related to the corresponding bottom level goals and the mapping follows a similar method, except for the lesson learned “Position Description: Define the sensitivity level” which could not be mapped to a FISCAM security requirement. This is probably because the existing goals, based on standards, guidelines and policies do not cover all aspects of an incident.

Step 4: Elaborate the Context and Strategy.

In the VA 2006 data leakage incident, as we have used the FISCAM as the basis for the decomposition of the goal, the strategy is stated as “Argument over FISCAM”. In this case, since there are some lessons learned that are not covered by the existing goal structure, they are mapped to a newly created goal named “Standard non-existent”. A new strategy named “Argument over all Missing Security Recommendations” is created and inserted between the top goal and the goal “Standard non-existent”.

The context notation is to provide supplementary information for a specific security incident. For example, we have explained the “FISCAM” in the strategy notation and the context is stated as “Federal Information Security Controls Audit Manual”.

Based on the steps above, the instance of the Generic Security Template for VA 2006 data leakage incident is presented in Figure 4.1. Five main lessons learned are derived from the VA 2006 data leakage incident report. Four of them were mapped to different levels of security requirements of FISCAM. One of them cannot be mapped to an appropriate security requirement, which indicates a probably missing aspect of the security guideline. The instance of the Generic Security Template for VA 2006 data leakage incident presents a security argument on how the security recommendations are gathered together to address the violated security requirements of the organisation. Compared to text-based incident reports, it may lose some details such as business impact information. However, it highlights the causes and recommendations, and the supportive relationships with the security requirements, which could help to improve the prevention of similar security incidents in the future.

4.2 Veterans Affairs (VA) data leakage incident 2007

4.2.1 Case description

“On January 22, 2007, a Veterans Health Administration (VHA) Information Technology (IT) Specialist assigned to the Research Enhancement Award Program (Birmingham REAP), VA Medical Centre (VAMC), Birmingham, AL, reported that a VA-owned external hard drive was missing from the REAP office. The missing external hard drive is believed to contain numerous research-related files containing personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the Centres for Medicare & Med-

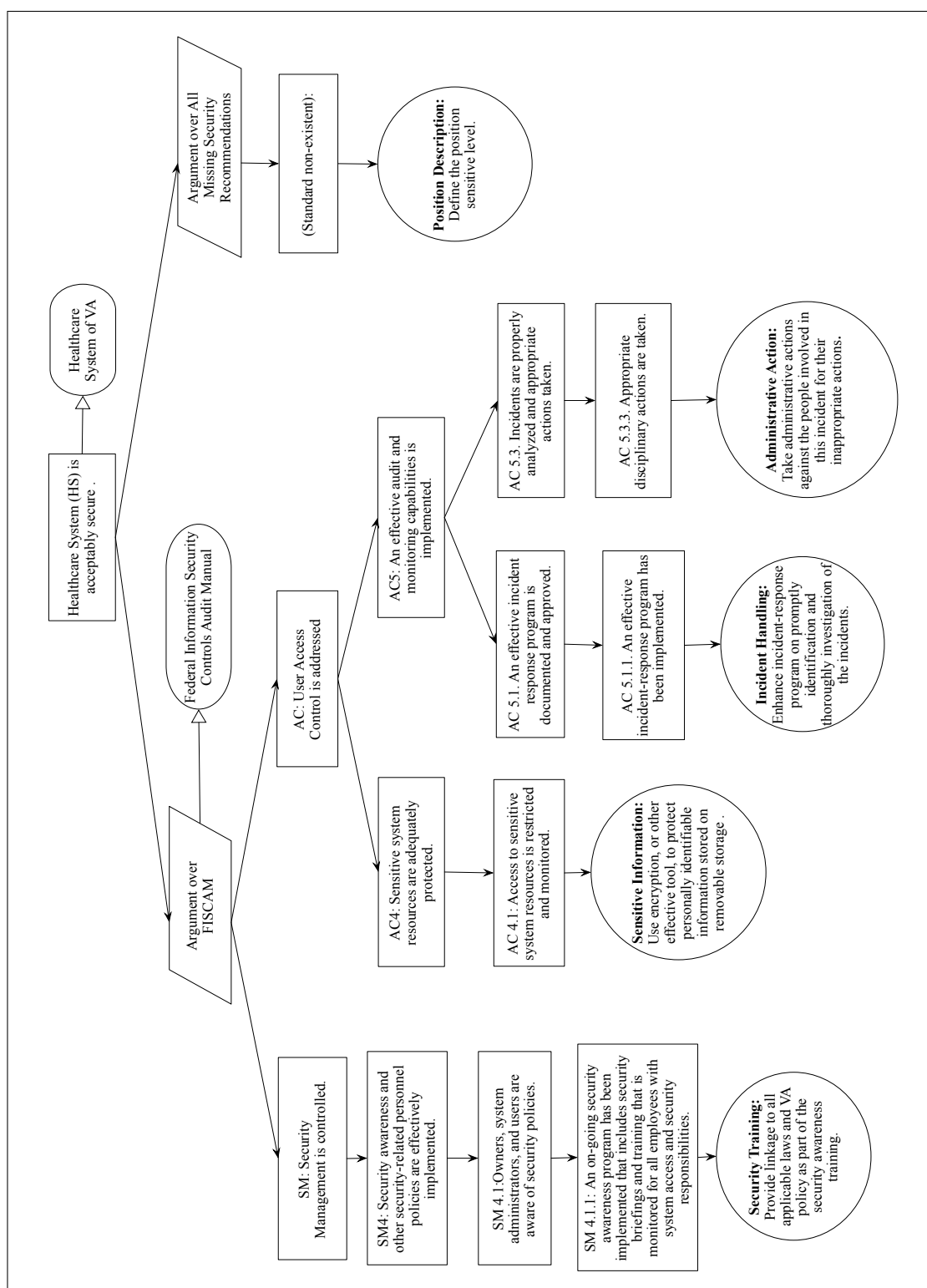


Figure 4.1: Instance of the Generic Security Template - VA 2006 data leakage incident

icaid Services (CMS), Department of Health and Human Services (HHS), on over 1.3 million medical providers. To date, the missing hard drive has not been recovered and there is no indication that the data on the missing external hard drive has been further compromised or used to commit Medicare fraud. Future investigation is conducted to identify the problem and recommendations are provided by VA office of Inspector General.” [15].

4.2.2 Instance of the Generic Security Template

Step 1: Prepare the goal structure.

Similar to VA 2006 data leakage incident, we have used the structured category of security requirements in FISCAM, specifically the general control section, as the goal structure for this security incident. Those goals form the goal structure for the VA 2007 data leakage incident.

Step 2: Identify the lessons learned.

The process of identification of the lessons learned (security issue and recommendation) is by looking for the learning points in the security incident report. The identified security issues and recommendations can be found in Table 4.5.

Table 4.2: Veterans Affairs (VA) data leakage incident 2007

Security Issues	Security Recommendations
Access Control	Avoid the abuse of programmer level access control.
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage
Security Policy	Ensure that data security plans for research projects comply with information security policies.
Security Policy	Ensure human subjects in research, compliance with information security requirements.
Security Policy	Discontinue storing email on unauthorised system.
Position Description	Re-evaluate and correct position sensitivity levels.

Table 4.2: (continued)

Security Issues	Security Recommendations
Management Structure	Establish a functional description and performance plan to clarify the line authority and reporting relationship.
Administrative Action	Take appropriate administrative actions against the people for their inappropriate actions.
Risk Analysis	Develop and issue Government-wide risk analysis criteria.

Step 3: Map the lessons learned to the goal structure.

The lessons learned identified are mapped to different levels of goals in the goal structure as before. However, we identified some difficulties when mapping the lessons to the security requirements in this security incident. We found that some lessons are related to more than one security requirements. For example, the lesson learned “Access Control: Avoid the abuse of programmer level access control” is found to be related to the goal “AC-3.1.1. Resource owners have identified authorized users and the access they are authorized to have” and “AC-3.1.2. Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs. (Standard naming conventions are essential to ensure effective configuration management identification and control of production files and programs vs. test files and programs)”. Reflecting all such relationships will make the diagram complicated. To keep the diagram concise, we suggest further guidance for mapping such lessons learned,

Starting from the bottom-level goals in the goal structure, if a lesson learned is related exclusively to a bottom-level goal, it should be mapped to this bottom-level goal. If a lesson learned is related to more than one bottom-level goals in the goal structure, this lesson learned should be mapped to the nearest parent goal where those bottom-level goals share the same parent goal.

According to this newly added guidance, this lesson learned should be mapped to the nearest parent goal where those bottom-level goals share the same parent goal, which is “AC-3.1. User accounts are appropriately controlled”. It indicates if this les-

son learned is ignored, the goal AC-3.1 or its sub-goals would be affected.

Step 4: Elaborate the Context and Strategy.

Since this security incident happened in the VA, the strategies and context information are the same, (i.e. the strategy is stated as “Argument over FISCAM”. The context used to explain the “FISCAM” in the strategy notation is stated as “Federal Information Security Controls Audit Manual”). Figure 4.2 presents the Generic Security Template built for VA 2007 data leakage incident.

In the VA 2007 data leakage incident, we have found two lessons learned that are similar to the VA 2006 data leakage incident with almost identical security issues and recommendations, which are “Sensitive Information” and “Administrative Actions”. It seems that VA has not effectively implemented the recommendations in VA 2006 data leakage incident to prevent them from recurrence. One lesson “Position Description” is found to have identical security issue but with different recommendations. It was recognised as a newly added aspect of the FISCAM in both GST instances, which indicates this lesson is probably a necessary aspect that is not covered by the security guideline. There are also some extra lessons found in this incident, which are “Access Control”, “Security Policy”, “Risk Analysis” and “Management Structure”. The same type of security incident, information data leakage incident, can have different causal issues behind it. As we could see, the use of the GST facilitates the comparison of similar incidents from organisations that apply the same security guidelines/standards.

4.3 Shenzhen data leakage incident 2008

4.3.1 Case description

In 2008, the healthcare information of pregnant women was disclosed from the hospital of Shenzhen, China. The criminals obtained up to 40, 000 items of medical information including the pregnant women’s name, baby’s birth date, home address, mobiles, etc. This information was updated monthly, adding up to 100, 000 items in total. The information was sold to businesses who were aiming to seize the market immediately after the new babies were born. These companies used the stolen data to push their sales such as first milk, baby sitter service, pregnant women fitness service, etc. through phone calls or messages. People were affected and felt offended by such

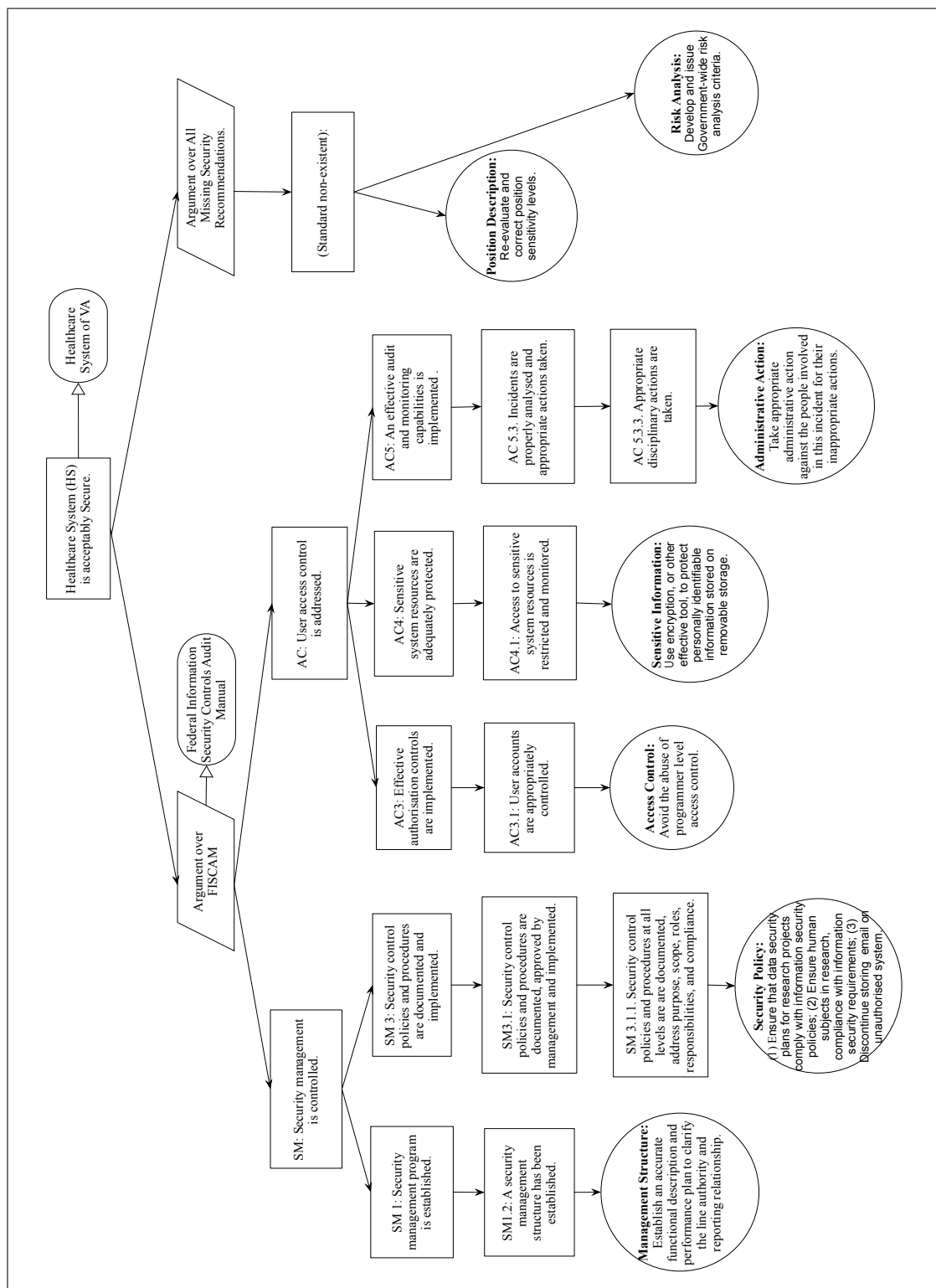


Figure 4.2: Instance of the Generic Security Template - VA 2007 data leakage incident

behaviours. The victims believed the data came from the profiles (names, mobiles, address, estimated birth date, etc.) they provided for registration in the hospital. Anyone accessible to the information can be suspicious in disclosing it to others and people are increasingly concerned about the security of healthcare system. Hospitals had just started the use of healthcare information system (HIS) in China. The managers were focusing more on its business functionalities rather than system security [16].

4.3.2 Instance of the Generic Security Template

Step 1: Prepare the goal structure.

As we are moving to healthcare organisation in China, the security standard we used is Information security technology - Baseline for classified protection of information system (GB/T22239). As mentioned in Chapter 2, it is required by the Ministry of Health of the People's Republic of China. The health information systems and its related units should be self-examined in accordance with GB/T22239. In particular, the tertiary (highest level) hospital needs to achieve at least the third level of the security standard.

Step 2: Identify the lessons learned.

Similar to VA 2006 and VA 2007 data leakage incident, the process of identification of the lessons learned (security issues and recommendations) is by looking for the learning points in the security incident report. The identified security issues and recommendations can be found in Table 4.3.

Table 4.3: Shenzhen data leakage incident 2008

Security Issues	Security Recommendations
Network Security	Network security needs to be ensured by following the security standards.
Sensitive Information	Define the information sensitive level according to the security standards.
Security Policy	Establish and enforce security policy according to the security standards.
Security Audit	Establish and conduct security audit plan according to the security standards.

Table 4.3: (continued)

Security Issues	Security Recommendations
Security Training	Establish and execute security training programs by following the security standards.

Step 3: Map the lessons learned to the goal structure.

Similar to VA 2006 and VA 2007 data leakage incident, the lessons learned identified from the Shenzhen case can be mapped to different levels of security requirements in the Chinese security standard GB/T22239.

Step 4: Elaborate the Context and Strategy.

As we are moving into the healthcare organisation in a different country, the strategy and context used are different. The strategy we used for justifying the decomposition is stated as “Argument over GB/T22239”. We have explained the “GB/T22239” in the strategy notation and the context is stated as “Security Standard China”.

Figure 4.3 presents the instance of the Generic Security Template built for Shenzhen 2008 data leakage incident. Five main lessons learned are identified. We have found three lessons learned are similar to the VA data leakage incidents, which are the issues “Sensitive Information”, “Position Description”, “Security Training”, but the recommendations are different. The recommendations in China seems more rigorously relying on the security standards. This can be justified by the immaturity of the healthcare information security management. The China healthcare organisation has just stated using the electronic healthcare record since 2008 and is relatively immature in information security management. Organisations tend to rely on the security standards as a starting point for shaping information security management strategy [59].

4.4 NHS Surrey IT Asset Disposal Incident 2013

4.4.1 Case description

“The Information Commissioner’s Office (ICO) has issued NHS Surrey with a monetary penalty of £200,000 after more than 3,000 patient records were found on a second hand computer bought through an online auction site. The sensitive information was inadvertently left on the computer and sold by a data destruction company employed

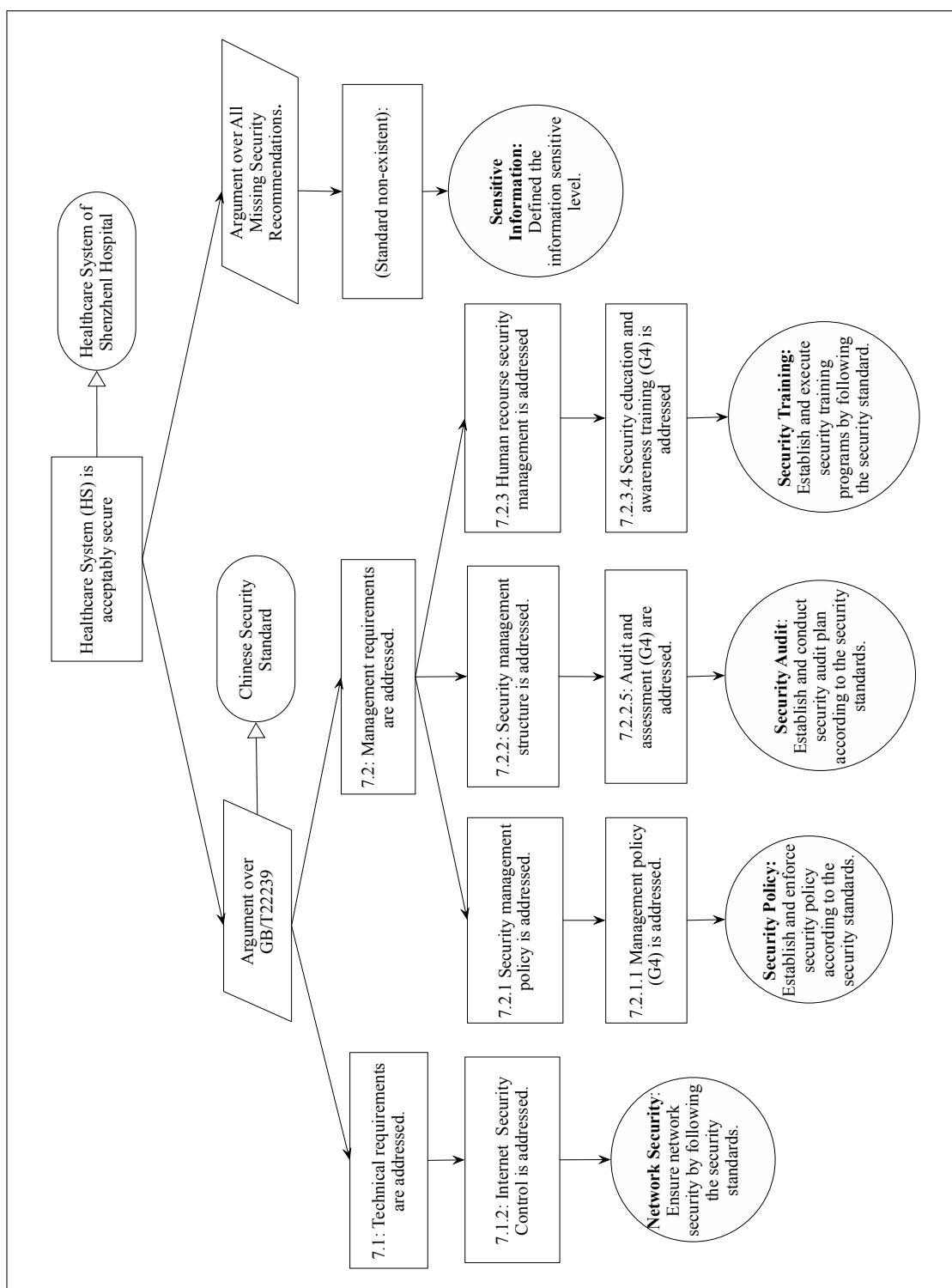


Figure 4.3: Instance of the Generic Security Template - Shenzhen 2008 data leakage incident

by NHS Surrey since March 2010 to wipe and destroy their old computer equipment. The company carried out the service for free, with an agreement that they could sell any salvageable materials after the hard drives had been securely destroyed. The ICO's investigation found that NHS Surrey had no contract in place with their new provider, which clearly explained the provider's legal requirements under the Data Protection Act, and failed to observe and monitor the data destruction process." [12].

4.4.2 Instance of the Generic Security Template

Step 1: Prepare the goal structure.

The Information Commissioner's Office (ICO) has provided the guideline [170] for IT asset disposal. This is part of a series of guidance, which goes into details than the main provision of the Data Protection Act (DPA) in the guide to data protection. It aims to help the data controller fully understand their obligations and promote good practices. It explains to the data controller what they need to consider when disposing of electronic equipment that may contain personal data. We have used this guideline as the goal structure of this security incident.

Step 2: Identify the lessons learned.

Similar to VA 2006, VA 2007 and Shenzhen 2008 data leakage incident, the process of identification of the lessons learned (security issue and recommendation) is by looking for the learning points in the security incident report. The identified security issues and recommendations can be found in Table 4.4.

Table 4.4: NHS Surrey IT Asset Disposal Incident 2013

Security Issues	Security Recommendations
Risk Management	Carry out a risk assessment when using a data processor to dispose of the hard drives.
Personal Data	Wipe medical information and confidential sensitive data before recycling.
Contract	Have a written contract with the company processing the IT Asset.

Table 4.4: (continued)

Security Issues	Security Recommendations
Disposal Monitoring	Monitor the destruction process and maintain audit trails and inventory logs of hard drives destroyed by the company based on the serial numbers in the destruction certificates for each individual drive.
Remedial Action	Take remedial action which includes developing a new policy framework to address the internal re-use of information and appliances and disposal process for redundant equipment.

Step 3: Map the lessons learned to the goal structure.

The lessons learned can have different levels of details to be mapped to different levels of security requirements in the security guideline, as in the previous case studies.

Step 4: Elaborate the Context and Strategy.

As we are moving into the healthcare organisation in UK, the strategy and context used are different. The strategy we used for justifying the decomposition is stated as “Argument over IT Asset Disposal Guidance”. We have explained the “IT Asset Disposal Guidance” in the strategy notation and the context is stated as “An IT Asset Disposal guidance proposed by Information Commissioner’s Office according to Data Protection Act”.

As is different from the previous cases happened in the US and China. This case study focuses on the IT asset disposal in the UK. Figure 4.4 presents the instance of the Generic Security Template built for NHS Surrey 2013 IT Asset Disposal Incident. Five main lessons learned are identified, that are related to the issue “Risk Management”, “Personal Data”, “Contract”, “Disposal Monitoring”, and “Remedial Action”. Among them, “Remedial Action” can not be mapped to an appropriate security requirement, which indicates a probably missing aspect of the the IT Asset Disposal guidance. The rest of them were mapped to different levels of security requirements of the IT Asset Disposal Guidance.

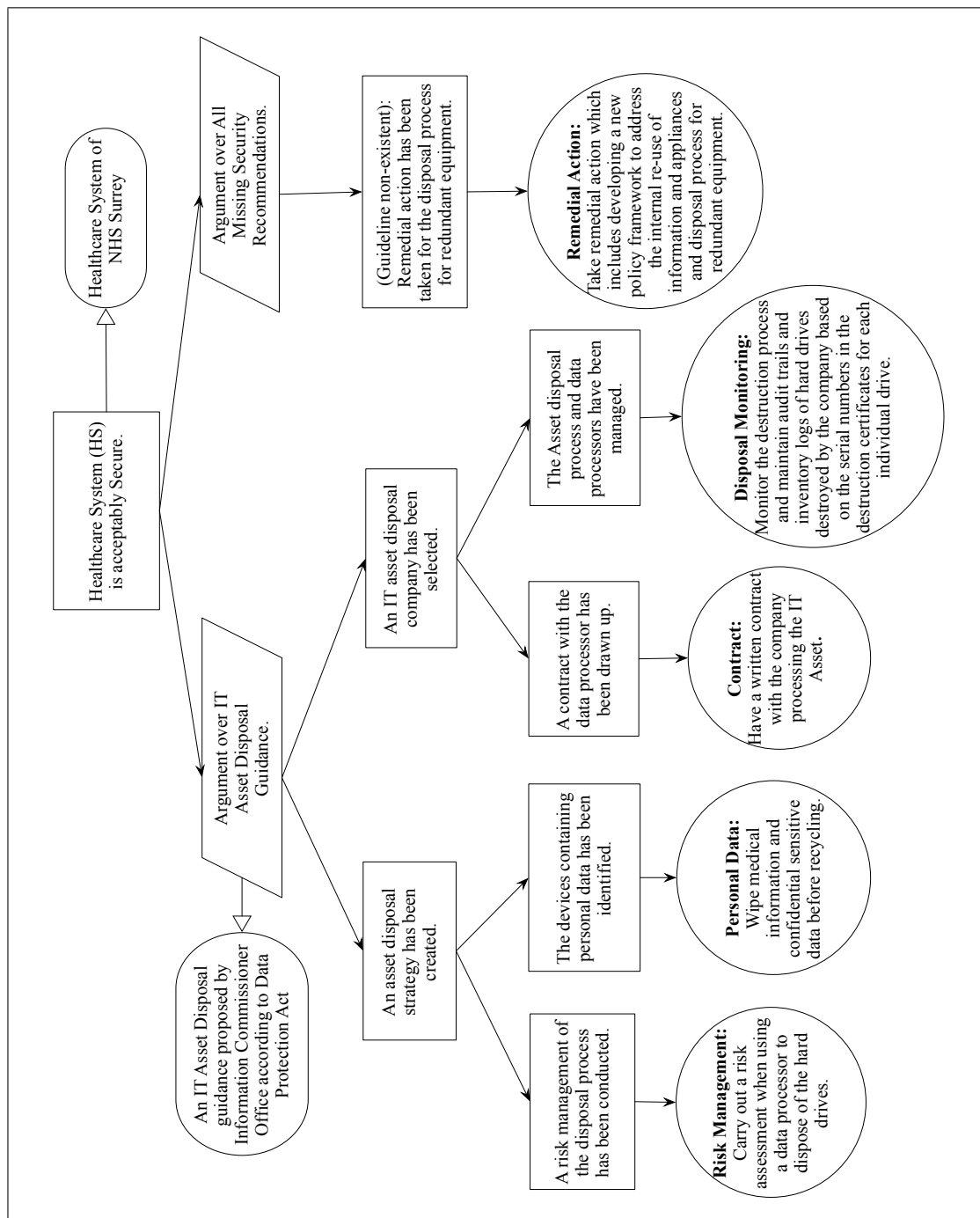


Figure 4.4: Instance of the Generic Security Template - NHS Surrey IT Asset Disposing

4.5 Discussion

4.5.1 Case selection

Security incidents happened in different industries such as telecommunication [171], finance [172, 173], healthcare [15] and government [174]. Information about incidents can be from a variety of data sources including security incident reports [14, 15], news clips [12, 172, 173], money penalty report [44] and so on. This research focuses on healthcare industry. The security incidents selected for case studies are representatives of healthcare security incidents happened in different countries (i.e. United States, UK and China).

In China, organisations are reluctant to release security incident reports. Information about incidents is limited and can only be obtained from news clips. Among 13 security incidents collected in China (Appendix A.5), only one incident is related to healthcare organisation, the Shenzhen data leakage incident [16]. Therefore, this incident is selected. Incident description in the new clips is usually free style text.

In the United States, some organisations release detailed security incident reports. For example, Department of Veterans Affairs Office of Inspector General has released reports on the review of Veterans Affairs (VA) security incidents. Incident description in the incident report is semi-structured text. Among 6 incident reports collected (Appendix A.5), two data leakage incidents are selected, VA data leakage incident 2006 [14] and 2007 [15]. It allows us to make comparisons with the Shenzhen leakage incident, which is of the same type. It also allows to make comparison between these two incidents happened in the same organisations.

In UK, information about security incidents can be found from Information Commissioner's Office (ICO). Among 14 incidents collected (Appendix A.5), five of them are related to healthcare. We selected the NHS Surrey 2013 IT Asset Disposal Incident [44] because it has a detailed money penalty report that documents the causes, recommendations and violated security requirements. Incident description in the incident report is semi-structured text. This allows us to model security incident from a different resource rather than news clips and security incident reports.

4.5.2 Success criteria

As is mentioned, the data sources of our selected case studies are diversified such as the official security incident reports used in the VA incidents, the news clip used in

the Shenzhen incident, and the money penalty report used in the IT asset disposing incident. The four case studies conducted in this chapter show that the GST can be used to structure the security lessons identified from a variety of data sources. The successfulness of this task is determined by the completion of each step to create the instances of the GST.

- In step 1, security requirements can be elicited based on the existing security standards applied by the organisation. There were no difficulties in completing step 1 as the security standards/guidelines are readily available to elicit security requirements.
- In step 2, lessons learned can be identified from different data source. Although incident description are from different data sources, lessons learned can be identified through content analysis [175] for those four case studies.
- In step 3, lessons learned can be mapped to the security requirements. Difficulties were found in step 3 while mapping the lessons learned with the security requirements. We overcome them by suggesting and adding new guidance to assist the creation process. However, the validity of the guidance needs to be further evaluated in real practice.
- In step 4, context and strategies can be elaborated for those instances. Strategies were elaborated and supplementary information can be extracted from incident descriptions as context for those instances.

4.5.3 Time and efforts

The creation of the instances requires the expertise of the analyst. The author conducted these case studies independently. The author has a computing science education background and five years research experience in information security incident management. Efforts can be measured in terms of time invested in each case study, as is shown in Table 4.5.

The time invested in those case studies varied. VA 2006 Data leakage incident consumes more time because the author needs to study the GSN and adjust it to fit into the needs of this research context. It was a combined efforts of experimental trials with GSN, security incident analysis, security guidance (i.e. FISCAM) review and GST instance modelling. With the experience gained from the first case study,

Security Incidents	Time	Efforts
VA 2006 Data Leakage	6 weeks	(1) Learning GSN related techniques (a month) (2) Read FISCAM (a week) (3) Read Security Incident Report (a week) (4) Create GST instance from Executive Summary (2 days)
VA 2007 Data Leakage	4 hours	(1) Create GST instance from Executive Summary (4 hours)
Shenzhen Data Leakage	3 days	(1) Read GB/T22239 (3 days) (2) Read incident news clips (30 minutes) (3) Create GST instance (2 hour)
NHS Surrey IT Asset	7 hours	(1) Read IT Asset Disposal Guidelines (2 hours) (2) Read Security Incident Report (2 hours) (3) Create GST instance (3 hours)

Table 4.5: Time and efforts to create the GST Instances

the author was able to complete the modelling of VA 2007 Data leakage incident very quickly. For the third case study, the author spent some time studying the security standard (i.e. GB/T22239) applied in Chinese healthcare organisation and was able to complete within approximately three days time. By following the same procedure, the author studied a fourth case study happened in the healthcare organisation in UK and was able to complete the study within 7 hours' time. An accurate measure of efforts invested requires further studies involving more users and case studies.

4.6 Summary

In this chapter, we presented four security incidents case studies from Europe, North America and China and produced four instances of the Generic Security Templates by following the instance creation steps introduced in Chapter 3. The creation of those instances has demonstrated the suitability of the Generic Security Template in presenting the lessons learned from the real world security incidents. In the following chapters, we evaluate the Generic Security Template by using those instances. In Chapters 5 and 7, we evaluate the usability of the Generic Security Template with university students. In Chapter 6 and 8, we industrially evaluate the Generic Security Template with people having experience dealing with patient data.

Chapter 5

Comparison of the Generic Security Template with traditional Text-based Approach - An Empirical Evaluation

Chapter 3 proposed the Generic Security Template; Chapter 4 tested the suitability of the Generic Security Template using a number of case studies. Since the Generic Security Template is created by using the graphical approach, the Goal Structuring Notations (GSN), there might be comprehension problems due to the usage of unfamiliar symbols. This chapter uses one instance of the Generic Security Template to empirically evaluate its usability in assisting the identification of lessons learned from security incidents in comparison to traditional free text approach.

This chapter is divided into the following sections. Section 5.1 introduces related work on the usability evaluation of graphical notations. Section 5.2 outlines the study design including the hypothesis, tasks, materials, pilot test, and study execution. Section 5.3 introduces the experiment procedures. Section 5.4 analyses the results quantitatively. Section 5.5 analyses the subjective feedback qualitatively. 5.6 discusses external and internal threats to the validity of the experiment. Section 5.7 discusses the findings, the contributions and limitations of the experiment. Section 5.8 summarises this chapter.

5.1 Related work

5.1.1 Graphical notation evaluation

Previous chapters argued that existing text-based reports can be supported through the use of graphical notations that provide an overview of many dozens of pages of detailed prose. Figure 5.1 uses the Goal Structuring Notation to summarise key findings from an enquiry into a leakage of confidential patient data from the US Veterans' Affairs Administration [15]. The aim is to present the security lessons in a structured and coherent manner. It is also hoped that this use of a semi-formal notation will encourage greater consistency and correctness [176, 177]. However, the notation introduces unfamiliar syntax and semantics. There is a danger that our use of these techniques can prevent stakeholders from understanding the arguments in security incident reports [178, 179]. This chapter, therefore, presents a controlled experiment to evaluate the utility of graphical representations for security incident reports.

There have been many previous studies into the utility and usability of graphical notations. For example, Razali has conducted an experiment comparing the comprehensibility of an UML-based graphical formal specification versus a purely textual specification [180]. Although graphical representations are often perceived as easier to understand, it can be difficult for readers to interpret the meaning of abstract symbols [181, 182]. Purely graphical representations are often less expressive than textual representation; in other words some system properties cannot easily be specified using diagrams alone [183]. It is for this reason that diagrams, such as that shown in Figure 5.1, resort to textual labels in addition to the graphical syntax. A combined graphical representation with supporting textual representations can assist visualisation while still achieving the full expressiveness and precision of a textual representation.

5.2 Experiment design

5.2.1 Experiment design and scope

A study was designed to evaluate whether the use of the Generic Security Template can help assisting the communication of lessons learned and security arguments on the supportive relationships between the lessons and the security requirements compared to conventional text-based approaches. The aim was not to show that the Generic Security Template could replace conventional reports; the focus was in the use of the

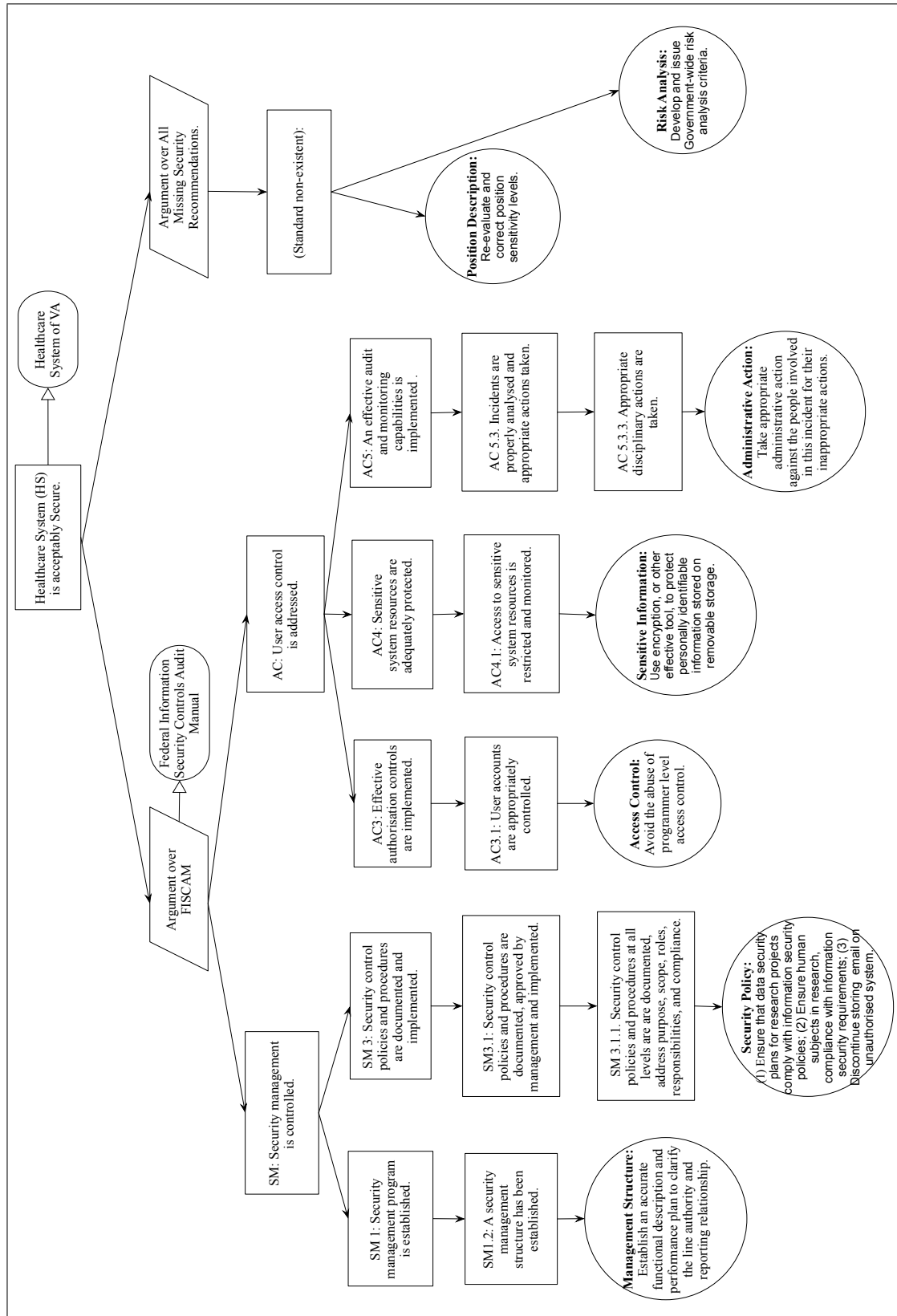


Figure 5.1: An example instance of the GST - VA 2007 data leakage incident

Generic Security Template to provide a map or overview of complex text-based reports. Accuracy, efficiency and task load are compared quantitatively in this experiment and the following hypotheses are proposed for the comparison.

H1 - Accuracy (Lessons Learned): Participants will be better able to identify the lessons learned (security issues, security recommendations) in security incident report with the help of the GST than using text-based documents alone;

H2 - Accuracy (Relationships between the lessons and the security requirements): Participants will be better able to identify the security arguments on the supportive relationships between the lessons and the security requirements with the help of the GST than using text-based documents alone;

H3 - Efficiency (Time): The time taken to complete the designed task will be less using the GST than using the text-based documents alone;

H4 - Task Load (TLX): The task load will be lower using the GST than using the text-based documents alone.

Ease of use is compared qualitatively based on the feedback obtained from participants.

5.2.2 Ethical approval

To conduct research involving human participants, this experiment adhered to the BPS ethical guidelines, and has been approved by the FIMS ethics committee of the University of Glasgow (ref: CSE01098) (Appendix B.1)

5.2.3 Experiment variables

5.2.3.1 Independent variables

Generic Security Template (GST), we have used one instance of the Generic Security Template, the VA 2007 data leakage incident, in this experiment as is shown in Figure 5.1.

Text-based approach, we developed an executive summary (reduced to four pages) (Appendix B.2) and a simplified security guidelines (reduced to three pages) (Appendix B.3) from the FISCAM.

5.2.3.2 Dependent variables

We were concerned to determine whether participants could use the graphical and textual versions of the report to identify the lessons learned and security arguments on the supportive relationships between the lessons and the security requirements. In particular, we evaluate its usability [184] in terms of the accuracy, efficiency, ease-of-use and task load compared to the conventional, text-based approach.

Accuracy, is measured by assessing the quality of the (1) lessons learned (security causes, recommendations) and (2) relationships between the lessons and the security requirements from the security incident.

Efficiency, is measured by the time it takes to complete the experiment task. Although time may not be a significant issue for many security concerns. If it takes too long to read and understand an incident report then it may dissuade some end users from investing the time needed to learn from previous incidents.

Ease of use, is evaluated by the feedback obtained from the post-experiment questionnaire.

Task load, is measured by the application of NASA's Task Load Index to assess workload [185].

5.2.3.3 Controlled variables

Participants, the participants were post-graduate and undergraduate students from UK. The use of the students is justified for pragmatic and also for ethical reasons. As part of this research, we conducted interviews with exiting healthcare and IT professionals in healthcare organisations (Chapter 6). This revealed that many lack formal training in security incident reporting and analysis; they come from varied backgrounds. The growing number of patient data breaches has also created enormous sensitivity; many employers are extremely unwilling to participate in studies of this nature even when anonymity is guaranteed.

Tasks, the experiment itself lasted for maximum one hour. Participants had to identify the lessons learned and the security arguments on the supportive relationships between the lessons and the security requirements using either a conventional text-based document or using the graphical overview plus the report.

5.2.3.4 Extraneous variables

Experience with GSN, is defined as an extraneous variable in this experiment. People who have experience with GSN will have an obvious advantage in understanding the security incident with the help of the GST. People having experience with GSN were excluded from this experiment.

5.2.4 Experiment material

5.2.4.1 Security incident related text document

The technical context of the task focused on a data leakage incident involving the Veterans Affairs' Administration [15]. The original report was around 80 pages long and hence we could not use it directly within the time available for the experiment. We also felt that our more focused approach was more appropriate for an initial study that could, in turn, inform future empirical work over a longer period of time and with a larger number of participants. We, therefore, reduced the executive summary from the VA report to four pages. As is mentioned, the security requirements to be supported by lessons learned are presented in the form of a specific security standard or guideline applied to the organisation where the security incident happened. Therefore, a simplified version of security guidelines (reduced to three pages) cited from the FISCAM that are relevant to this incident are also provided as a part of the security incident report.

5.2.4.2 The Generic Security Template (GST)

The instance of the GST, as is shown in Figure 5.1, used in this experiment is created from the above mentioned security incident related document only. It is an abstraction and extraction of the desirable information and did not bring any information from other sources that could potentially bias the results of the experiment.

5.2.4.3 The questionnaire

We developed separate tasks description for the two groups and a post-experiment questionnaire, to provide subjective insights into perceived workload. A slightly different version of this post-experiment questionnaire was developed for the group using the graphical overview of the security incident. They were asked to provide information about the usability of the approach by completing the subjective questionnaire.

5.2.5 Pilot study

Two security experts reviewed the design of the experiment pilot studies and helped to identify issues that had not been identified during the preparation of the materials. These included the clarity of the instruction, the validity and complexity of the tasks and the practicality of the tasks required relative to the time available for the experiment. In the first pilot study, participants had to identify security issues, recommendations and security arguments on the supportive relationships between the lessons and the security requirements; writing them down using freestyle text. This was to simulate how security incident reports are analysed in practice, where people normally have no tools assisting them throughout this process. The feedback from the participants showed that the task was very mentally demanding and they were not able to complete it within one hour. We corrected this problem by introducing a table that provided guidance on the security issues and recommendations. Table 5.1 is an exempt of the table. Issue category and description are provided. The participants need to fill in the blank about the recommendation description.

Issue Category	Issue description	Recommendations description
Access Control Related	The IT Specialist was improperly given access to multiple data sources.	

Table 5.1: An exempt of the security issue and recommendation table

For the measurement of the relationships between the lessons learned and the security requirements, we used multi-choice questions as the measurement. Below is an example,

What are the security recommendations for addressing the security requirement “User Access Control”?

a. Develop and implement policies describing the conditions under which programmer level access may be granted for research purposes.

b. Effective procedures are implemented to determine compliance with authentication policies.

c. Attempts to log on with invalid passwords are limited. Use of easily guessed passwords (such as names or words) is prohibited.

d. None of the above

Although this significantly reduced the workload in our study, it illustrated the more general problems that arise when individuals were asked to identify key findings from existing security incident reports. Two more participants conducted a pilot test of the new experiment design. They were able to finish the tasks and stated that the level of mental effort was acceptable. Experiment materials including an Information Sheet, Consent form, Task Sheets and the Post-experiment Questionnaires were also reviewed to identify any missing or ambiguous questions and instructions.

5.2.6 Experiment task design

We were concerned to use an incident report that typifies some of the barriers that dissuade security managers from reading existing recommendations. We, therefore, extracted key sections from the VA mentioned earlier [15]. Even so, a pilot study revealed that participants found it difficult to identify causes, recommendations, and the relationships between the lessons learned and security requirements in the abridged report about the pilot study also raised concerns about task load, fatigue and learning effects; which will be discussed in the following paragraphs.

In Group A, the experiment materials included the textual incident document (reduced executive summary and reduced security guidelines from FISCAM), the graphical GST and a task description. The pilot study had confirmed the arguments presented in the opening sections of this chapter; that it can be difficult for readers to identify the causes, recommendation and their relationships with the security requirements of previous security incidents from existing textual reports. We, therefore, created tasks that guided the participants' analysis:

Task 1: Identify security lessons from the security incident report with the help of the GST. They had to complete missing information from a table that provided partial information about the causes and recommendations, as is shown in Table 5.1.

Task 2: Answer multiple-choice questions about the security arguments on the supportive relationships between the lessons and the security requirements. This removed the additional contextual support of the tabular format used in task one and provided a stepping stone towards the open-ended analysis of security incident reports that proved problematic in the pilot studies.

In Group B, the experiment materials included the textual incident report without the GST but participants had the same task descriptions as the first group.

The methods used in task 1 and task 2 raised numerous further questions. Task

1 used open-ended questions. The scoring of open-ended responses is more difficult and less clear-cut. One must establish criteria for the kinds of answers that will be counted as correct; there is usually (if not always) at least some subjective judgment of the correctness of participants' responses. Dewar pointed out that the extra effort is worthwhile in terms of information gained about the types of errors and confusions people make and might assist in any subsequent redesign work [186]. Task 2 used multiple-choice questions to examine the participants' ability to identify the security arguments on the supportive relationships between the lessons and the security requirements. However, this approach raises concerns about the quality of the distracters (wrong answers), which could greatly influence comprehension scores [186]. Using a between group design with identical tasks enables an assessment of the support provided by the GST overview. However, the study also provided significant insights into the methodological issues associated with work in this area. In particular, we employed multiple independent security experts in the evaluation process, especially when participants were free to complete the information requested in Task 1 using their own terminology.

5.3 Experiment procedures

5.3.1 Experiment treatment

There was only one treatment in the experiment using a between groups (Group A and B) design. The empirical comparisons are between one group using a conventional text-based document and another using the graphical overview as well as the existing report. We have not used cross-over trials [187] in the experiment, because (1) the task was complex and time consuming that had taken approximately two hours, which was confirmed from the pilot study. The participants can experience fatigue through cross-over trial, as it doubles the task load. However, it is impossible to reduce the task load to allow a cross-over test, because this experiment aims to reflect the security incident comprehension process. Simplification of the experiment tasks will undermine the significance of the study; (2) None of the participants have previous experience in analysing security incidents. There can be a learning effect using the cross-over tests; (3) In a cross-over trial, two security incidents with similar complexity were needed. It was difficult to measure this complexity accurately. Therefore, we conduct one treatment in the experiment.

5.3.2 Participants

As mentioned, we were concerned to assess the participants' ability to use textual and graphical incident reports to identify lessons from previous data breaches. In consequence, the tasks required about one hour to complete. This limited the number of participants during our initial evaluation. Twenty-four subjects were randomly assigned to either of the two experimental conditions using the textual report only or using both the textual report and the graphical overview. Group A consists of one undergraduate student and eleven postgraduate students, within which three of them have information security experience; Group B has one undergraduate student and eleven postgraduate students, within which three of them have information security experience. Each of the groups have three females and nine males.

5.3.3 Training of the participants

A pre-scripted familiarisation tutorial was provided before the experiment. Participants from both Group A and B attended the same tutorial session. This was to ensure that they received equal knowledge related to the handling of security incidents. The participants were introduced to the GSN and GST.

5.3.4 Experiment execution

The experiment was conducted on a one-to-one mode to provide any support needed during the whole process including the familiarisation tutorial session, the experiment session and the post-experiment questionnaire session. During the familiarisation tutorial session, the participant had unlimited time to study the material and to have any question clarified. The participants were allowed to refer to the tutorial document or notes. The participants were instructed to inform the conductor if they had any trouble in understanding the questions. After the post-experiment questionnaire session, an informal interview was conducted to make sure their attitudes were consistent with the answers they have provided. They were also requested to write down their subjective feedback on the GST.

5.3.5 Analysing the data

5.3.5.1 Scoring Scheme for the experiment tasks

To reduce the bias, sample answers for the experimental tasks were agreed on by the research conductor and an independent security expert (Expert A).

5.3.5.2 Preparation for task 1 - open-ended questions

For Task 1, the answers were qualitative. The marking was based on the description of security issues and recommendations expected from the sample answers. The answers for each task were marked by two further independent experts (Rater A and B) using an agreed scoring scheme. Both Rater A and B are the author's colleagues from School of Computing Science in University of Glasgow and they are from an information security background. Rater A has over 20 years experience in information security and Rater B has six years experience in information security.

The participants' answers were classified into four categories, which are "Correct", "Incomplete", "Wrong" and "Blank". A correct answer completely described the recommendation to support the given issue; incomplete answers show that the participant had a partial understanding of the recommendation, but lacked comprehension of an important aspect of it. Wrong answers showed that the participant did not understand a particular recommendation. Blank, no answer was provided at all. The following paragraph provides an example from task one:

The report identifies the security concern: "The IT Specialist was improperly given access to multiple data sources". An answer is marked as, *Correct*, if the participant states that the recommendation associated with this issue was to "Consider the conditions under which programmer level access may be granted for research project". A correct answer completely describes the recommendation to support the given issue; *Incomplete*, if the answer is stated as "Ensure the access control is appropriately granted". Incomplete answers showed that the participant had a partial understanding of the recommendation, but lacked comprehension of an important aspect of it; *Wrong*, if the answer provided is not relevant to a particular recommendation. *Blank*, if no answer was provided at all.

Each participant was free to use his or her own words to describe the recommendations in this part of the study. The group identifiers were removed so that Rater A and B marked the answers without knowing whether or not the participants had access to the GST diagram.

5.3.5.3 Preparation for Task 2 - multi-choice questions

Task 2 used multi-choice questions to examine the participant's ability in understanding the compliance with the security requirements. Less subjectivity was involved in interpreting the answers. There can be more than one correct choice for each question and participants were asked to select all of the responses they believe were relevant to the questions. Below is an example,

What are the security recommendations for addressing the security requirement "User Access Control"?

- a. Develop and implement policies describing the conditions under which programmer level access may be granted for research purposes.*
- b. Effective procedures are implemented to determine compliance with authentication policies.*
- c. Attempts to log on with invalid passwords are limited. Use of easily guessed passwords (such as names or words) is prohibited.*
- d. None of the above*

Correct answer: a, b

The sample answers were prepared by the independent security expert A. Each answer was classified as, *Correct*, *Broad*, *Incomplete*, *Incomplete and broad*, *Wrong*, and *Blank*. A *Correct* answer contained and only contained all the acceptable choices (e.g. a, b); *Broad* contained all the acceptable choices, but also incorrect choices (e.g. a, b, c); *Incomplete* answers contained only some of the acceptable choices but not all (e.g. a). *Incomplete and broad* answers contained some of the acceptable choices and also other choices. (e.g. a, c); *Wrong* answers contained none of the acceptable choices (e.g. c). There was only one blank answer out of 144 responses.

5.4 Results

5.4.1 Results for accuracy (lessons learned)

Out of a total number of 168 answers to the seven questions in task 1 by 24 participants, three were left blank with one in Group A and two in Group B. During the debrief, the participants stated that, for the blank response, they could understand the questions

but they are not really interested to find the answer for those questions. Therefore, we ignore these blank answers in the subsequent analysis.

5.4.1.1 Comparing the performance of task 1

Since the results are categorical data, we use cross-tabulation analysis to analyse the results. A data set with 168 rows was imported into SPSS. Within the cross-tabulation analysis, groups were set as rows and task results were set as columns. Chi-square statistics was selected to test the hypothesis. Recall that these open ended questions were assessed by two independent raters. For Rater A, as is shown in Table 5.2, the results from the cross-tabulation analysis show that 62.7% of the responses from Group A were correct, which is 18.8% higher than Group B. This might seem a relatively low level of accuracy. However, it is important to recall that our marking scheme was careful to distinguish between complete, perfect responses and partially correct or incomplete answers. The total percentage of incomplete and correct answer is 81.9% in Group A, which is 16% higher than Group B. As is shown in Table 5.3, the Chi-Square Test ($P = 0.031 < 0.05$) shows that these results are statistically significant. Therefore, hypothesis H1 “Participants will be better able to identify the recommendations and causes in security reports with the help of a graphical method than using text alone” is supported based on Rater A’s judgement.

		Task			Total
		<i>Wrong</i>	<i>Incomplete</i>	<i>Correct</i>	
Group A	Count	15	16	52	83
	% within Group	18.1%	19.3%	62.7%	100.0%
Group B	Count	28	18	36	82
	% within Group	34.1%	22.0%	43.9%	100.0%
Total	Count	43	34	88	165
	% within Group	26.1%	20.6%	53.3%	100.0%

Table 5.2: The performance of Task 1 using Cross-tabulation by Rater A

For Rater B, as is shown in Table 5.4, the results from the cross-tabulation analysis show that 65.1% of the responses from Group A were correct, which is 20% higher than Group B. The total percentage of Incomplete and Correct answer is 83.1% in Group A, which is 9.6% higher than Group B. As is shown in Table 5.5, the Chi-Square

	Chi-Square Tests		
	<i>Value</i>	<i>df</i>	<i>Asymp. Sig. (2-sided)</i>
Pearson Chi-Square	6.951a	2	.031
Likelihood Ratio	7.029	2	.030
Linear-by-Linear Association	6.909	1	.009
N of Valid Cases	165		

Table 5.3: Chi-Square Tests performance of Task 1 using Cross-tabulation by Rater A

Test ($P = 0.019 < 0.05$) shows that these results are statistically significant. Therefore, hypothesis H1 “Participants will be better able to identify the recommendations and causes in security reports with the help of a graphical method than using text alone” is again supported based on Rater B’s judgement.

		Task			Total
		<i>Wrong</i>	<i>Incomplete</i>	<i>Correct</i>	
Group A	Count	14	15	54	83
	% within Group	16.9%	18.1%	65.1%	100.0%
Group B	Count	28	17	37	82
	% within Group	34.1%	20.7%	45.1%	100.0%
Total	Count	42	32	91	165
	% within Group	25.5%	19.4%	55.2%	100.0%

Table 5.4: The performance of Task 1 using Cross-tabulation by Rater B

5.4.1.2 Inter-rater reliability

Since these open ended questions were assessed by two independent raters, inter-rater reliability was checked for each question in Task 1. As is shown in Table 5.6 - 5.12, the Kappa Agreement shows that the two raters have achieved agreements on judging the accuracy of the lessons learned identified by the participants and the results are statistically significant (*Approx.Sig.* < 0.001). Landis and Koch proposed the benchmark scale on how the extent of agreement among raters should be interpreted and how the extent of agreement among raters should be interpreted, as is shown in Table 5.13 [8]. They have recommended this as useful guideline and Everitt also supported this bench-

	Chi-Square Tests		
	<i>Value</i>	<i>df</i>	<i>Asymp. Sig. (2-sided)</i>
Pearson Chi-Square	7.962a	2	.019
Likelihood Ratio	8.071	2	.018
Linear-by-Linear Association	7.911	1	.005
N of Valid Cases	165		

Table 5.5: Chi-Square Tests performance of Task 1 using Cross-tabulation by Rater B

mark scale [188]. Questions 1, 2 have achieved “almost perfect agreement”; Questions 3, 4, 5, and 6 have achieved “substantial agreement”; Question 7 has achieved “Fair agreement”.

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.706	.117	4.254	.000
N of Valid Cases	24			

Table 5.6: Inter-rater reliability for Task1 Question 1 (Rater A and B)

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.801	.105	5.415	.000
N of Valid Cases	23			

Table 5.7: Inter-rater reliability for Task1 Question 2 (Rater A and B)

5.4.2 Results for accuracy (security arguments)

As is shown in Table 5.14, the results from the cross-tabulation analysis show that the participants from Group A achieved a 33.3% accuracy rate, which is 9.7% higher than Group B. The total percentage of Correct, Broad, Incomplete, and Incomplete but broad answer is 87.5%, which is 18.1% higher than Group B. As is shown in Table 5.15, the Chi-Square Test ($P = 0.038 < 0.05$) shows that these results are statistically significant. Therefore, hypothesis H2 “Participants will be better able to identify the

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.715	.127	4.786	.000
N of Valid Cases	24			

Table 5.8: Inter-rater reliability for Task1 Question 3 (Rater A and B)

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.574	.128	3.962	.000
N of Valid Cases	22			

Table 5.9: Inter-rater reliability for Task1 Question 4 (Rater A and B)

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.723	.120	4.796	.000
N of Valid Cases	24			

Table 5.10: Inter-rater reliability for Task1 Question 5 (Rater A and B)

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.782	.104	5.325	.000
N of Valid Cases	24			

Table 5.11: Inter-rater reliability for Task1 Question 6 (Rater A and B)

Symmetric Measures				
	<i>Value</i>	<i>Asymp.Std. Error a</i>	<i>Approx. Tb</i>	<i>Approx. Sig.</i>
Measure of Agreement Kappa	.497	.154	3.251	.001
N of Valid Cases	24			

Table 5.12: Inter-rater reliability for Task1 Question 7 (Rater A and B)

Landis and Koch-Kappa's Benchmark Scale	
<i>Kappa Statistic</i>	<i>Strength of Agreement</i>
< 0.0	Poor
0.0 to 0.20	Slight
0.21 to 0.40	Fair
0.41 to 0.60	Moderate
0.61 to 0.80	Substantial
0.81 to 1.00	Almost Perfect

Table 5.13: Landis and Koch-Kappa's benchmark scale [8]

security arguments on the supportive relationships between the lessons and the security requirements with the help of the GST than using text-based document alone;" is supported in Task 2.

		Task					Total
		<i>Wrong</i>	<i>Incomplete and broad</i>	<i>Incomplete</i>	<i>Broad</i>	<i>Correct</i>	
Group A	Count	9	11	19	9	24	83
	% within Group	12.5%	15.3%	26.4%	12.5%	33.3%	100.0%
Group B	Count	22	4	18	11	17	82
	% within Group	30.6%	5.6%	25.0%	15.3%	23.6%	100.0%
Total	Count	31	15	37	20	41	165
	% within Group	21.5%	10.4%	25.7%	13.9%	28.5%	100.0%

Table 5.14: The performance of Task 2 using Cross-tabulation

5.4.3 Results for efficiency (time)

The mean total time used by Group A was almost equal with that in Group B; 47.3 versus 47.8 minutes. The total time taken across all tasks is not statistically significant ($P = 0.932 > 0.05$). Therefore, we can accept the null hypothesis that "the mean time taken to complete our experimental tasks using a textual security incident report and a textual report with a graphical overview are not significantly different". Hypothesis H3 is not supported. One interpretation of these results is that significant time is required to understand security incidents, irrespective of whether they are presented in graphical or textual format. However, this would require further empirical support to determine whether or not other graphical notations might lead to significant differences in the

	Chi-Square Tests		
	<i>Value</i>	<i>df</i>	<i>Asymp. Sig. (2-sided)</i>
Pearson Chi-Square	10.140a	4	.038
Likelihood Ratio	10.449	4	.034
Linear-by-Linear Association	2.995	1	.084
N of Valid Cases	144		

Table 5.15: Chi-Square Tests performance of Task 2 using Cross-tabulation

time taken to understand security incident reports. It is also important for further work to consider the learning effects that might be expected through repeated use of the Generic Security Template.

5.4.4 Results for task load index (TLX)

We used NASA's Task Load Index [185] to assess workload using a post-evaluation questionnaire. The t-test results show a significant difference ($P = 0.047 < 0.05$) in the first dimension of the task load index regarding "how mentally demanding was the whole task". With a mean value of task load, 12.75 versus 15.50, participants expressed a lower subjective level of workload in terms of "mentally demand" when using the GST. An interpretation of this results might be the linkage of data within the diagram has helped reduced the participants' mental efforts. The results for the other four dimensions of the Task Load Index are not significantly different. However, a more sustained analysis is required to replicate these findings across a wider range of workload measures and with a larger sample of potential users.

5.5 Subjective feedback

This section qualitatively analyses the subjective feedback from the experiment. As is shown in Table 5.16, the questionnaire included six sections. Section 1 and Section 2 are designed for both Group A and Group B. Section 1 collects background information about the participants. Section 2 collects participants' feedback on task load. Section 3 is designed for Group A for collecting subjective feedback regarding the usability of the GST using Cognitive Dimensions of Notations Usability Framework [189]. Section 4 is designed for Group A to collect subjective feedback on the overall

experience of the GST. Section 5 is designed for Group B to collect subjective feedback on the overall experience of the Security Incident Report. Section 6 is designed for Group B to collect subjective feedback on the GST.

Table 5.16: Questionnaire sections that belong to Group A and Group B

Questionnaire	Group A	Group B
Section 1: Demographic Information	X	X
Section 2: Task Load Index	X	X
Section 3: Cognitive Dimension	X	
Section 4: Feedback of the experiment with the Generic Security Template	X	
Section 5: Feedback of the experiment with Text-based approach		X
Section 6: Feedback of the Generic Security Template		X

5.5.1 Evaluation using Cognitive Dimensions

Section 3 of the questionnaire was based on the analytical theoretical framework Cognitive Dimensions of Notations Usability Framework [189]. This approach has been assessed for validity and reliability by a number of other researchers [190–192]. There are fourteen dimensions in the full framework. For our study, we did not ask about the creation or modification of the notation.

Example:

(Visibility) It is easy to see or find the various parts of the Generic Security Template while it is being used?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain what kind of things is difficult to see or find?

Questionnaire Section 3 provided preliminary results of the strengths and weakness of the GST used under certain circumstance, for example, any strength that the

user is in favour of, any weakness that affects usability, any opportunity for further improvements.

CD-Visibility Dimension. Ten out of twelve of the participants agreed or strongly agreed that “It is easy to see or find the various parts of the GST while it is being used”. One participant disagreed and argued about the visibility of the goal structure. The comment was “might be difficult to differentiate between goals and sub goals”. The suggestions were “use of colour may help visual interpretation” and “introduction of colours to identify the different levels/layers”.

CD-Diffuseness Dimension. Eleven out of twelve of the participants agreed or strongly agreed that “the GST lets you say what you want reasonably brief”. There was one participant against it and the reason was “too many words”. This issue is related to the level of abstraction of the GST. Too much information will undermine the effectiveness of the graphical presentation, while too little information will make it difficult to understand. Since a large proportion of the participants were pleased with the current design, we decided not to make any changes.

CD-Hard Mental Operation Dimension. Six out of twelve of the participants disagreed that “There seem some things especially complex or difficult to understand in your head while using the GST”. Two out of twelve of the participants agreed or strongly agreed and stated this was caused by “too many words within one notation”. They suggested to “separate recommendation into different or individual circles”. This issue relates to the separation of the lessons learned notation. We have accepted this recommendation by separating the notation that has more than one learning points. For example, the “Security Policy: (1) Ensure that data security plans for research projects comply with information security policies; (2) Ensure human subjects in research, compliance with information security requirements; (3) Discontinue storing email on unauthorised system” can be separated into three individual lessons which are “Security Policy: Ensure that data security plans for research projects comply with information security policies”, “Security Policy: Ensure human subjects in research, compliance with information security requirements”, and “Security Policy: Discontinue storing email on unauthorised system”.

CD-Closeness of Mapping Dimension. Nine out of twelve of the participants agreed or strongly agreed that “the GST describes the problem accurately and completely for the security incident stated in the textual document”. There was one participant against it and the feedback was “the case is not generic enough”, this is consistent with the comments on CD-Hard Mental Operation Dimension “with many words”.

The participants also argue about separation of the recommendation notations, “it’s in some cases hard to separate the individual solutions in one bottom node into separate issues”, which had some overlap with the finding in the CD-Hard Mental Operation Dimension. This issue relates to the separation of the lessons learned notation. As is mentioned earlier, we have accepted this recommendation by separating the learning points more carefully.

CD-Consistency Dimension. Seven out of twelve of the participants disagreed that “There are places where some things ought to be similar, but the GST makes them different”. Three out of twelve of the participants agreed or strongly agreed with it but there were no comments or suggestion related to this usability dimension.

CD-Role Expressiveness Dimension. Seven out of twelve of the participants agreed or strongly agreed that “while reading the GST, it is easy to tell what each part is for in the overall scheme”. One participant disagreed with it. The feedback was “might be hard to see whether the user wants to work on the high or low level of the hierarchy”. They suggested that “could use multiple cases” for different target groups with interest towards different level of information. This issue needs to be addressed in future industrial evaluation regarding multi-view to reflect the needs of different target groups such as security managers, engineers and so on.

5.5.2 Overall experience

Figure 5.2 shows that in Group A, approximately half of the participants expressed some difficulties in understanding the text based security incident report. Half of the participants reported that they have no difficulties in identifying security lessons learned from the security incident report with the help of the GST. Figure 5.3 shows that Group B demonstrated a slightly higher level of understanding of the security incident report. However, more than half of the participants had difficulties in identifying security lessons from the security incident report. These subjective findings are consistent with the quantitative results in section 6.3 that the group with GST are better able to identify the security lessons than the other.

The participants’ answers to the open questions regarding the overall experience of using the graphical overviews suggested that a longer training session might have helped them to better prepare for the tasks. Several participants mentioned that they had experienced learning effects; their confidence in answering the questions increased as they worked their way through the questions. This finding from Group A reveals

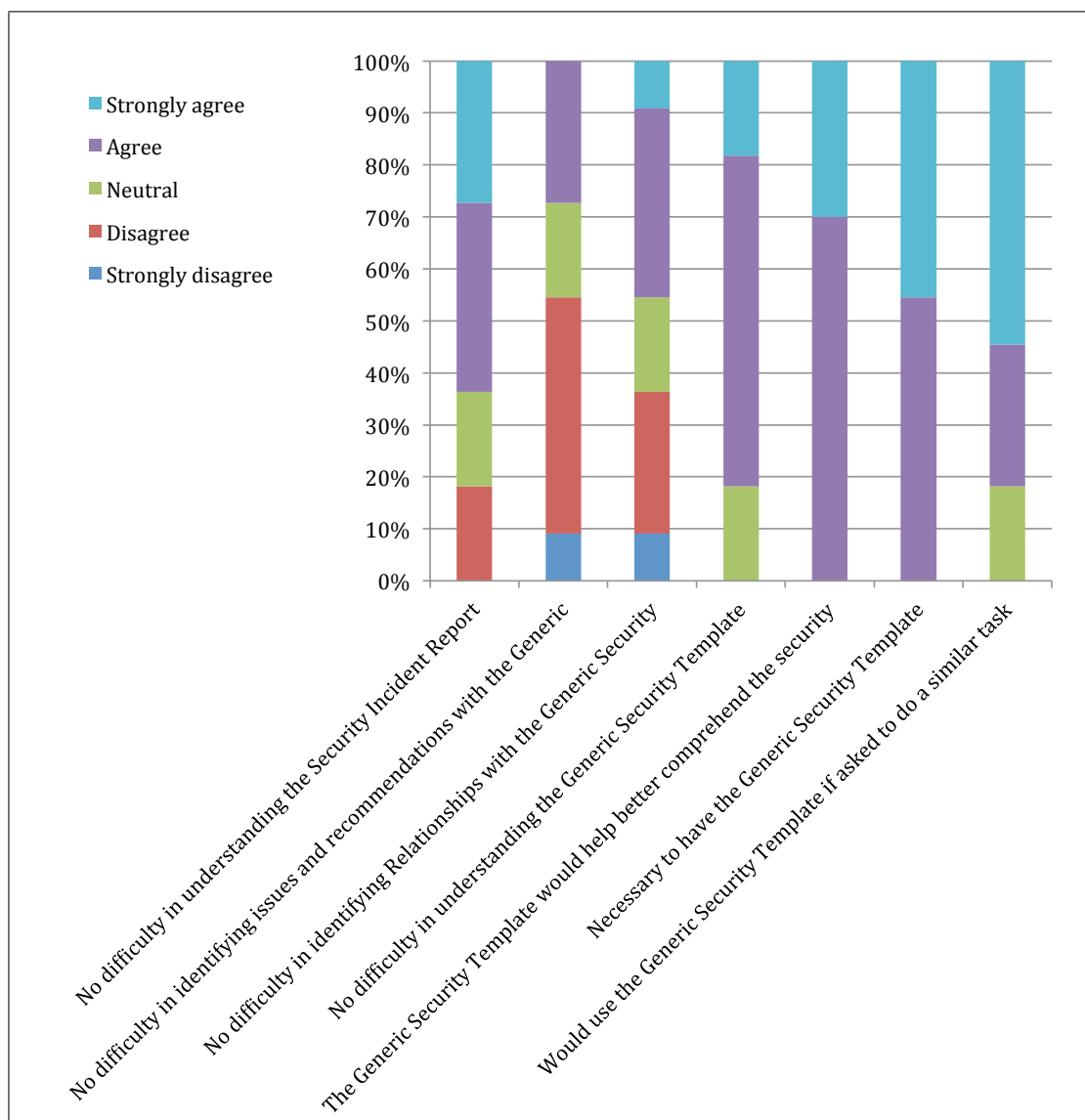


Figure 5.2: Overall experience of the GST - Group A

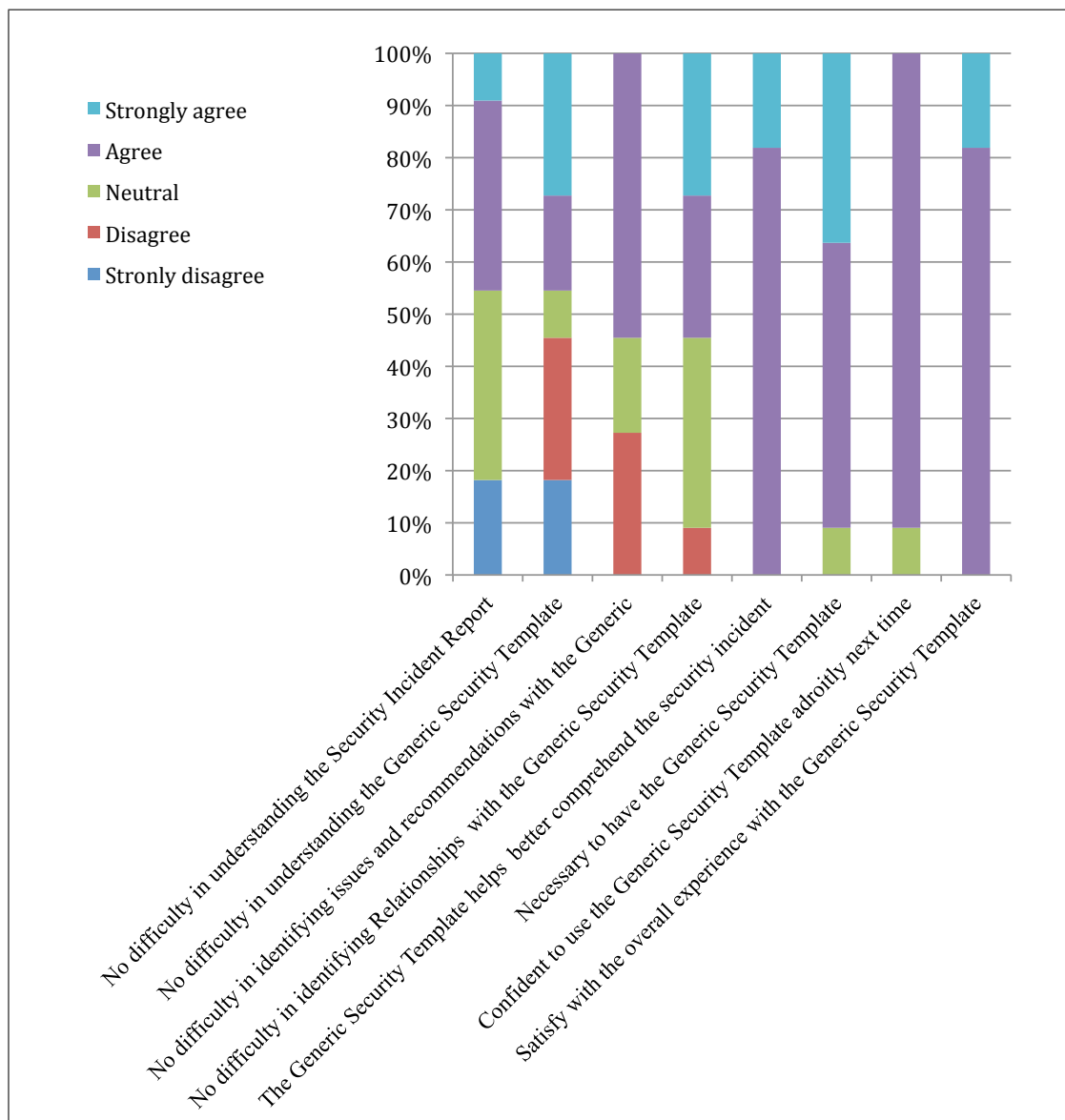


Figure 5.3: Overall experience of the GST - Group B

generally positive feedback for the GST. Group B did not use the GST during the experiment. They were, however, asked to review the GST after the experiment and provide the feedback by completing Questionnaire Section 6 designed for Group B. Almost all of them suggested that they would have no difficulties in understanding the GST and agreed that the GST can help them better comprehend existing security incident reports. Two thirds of the participants reported their willingness to use the GST if they are requested to do a similar task in the future. “It will help to understand terminologies security lessons, less confusing, very structured and don’t have to waste time, most importantly very easy to understand with less information”. In summary, the participants’ overall experience with the GST is positive, however, questions remain about the ability of people to apply the lessons from the report within their own organisation rather than answering direct questions about the contents of a security report.

5.6 External and internal threats

Threats to validity [193] are factors other than the independent variables that can affect the dependent variables.

5.6.1 Internal validity

Internal validity is concerned about the cause-effect relationships induced from the study. *Maturity effects*, there is a threat that the participants would tend to be bored and performed worse towards the end of the experiment session. However, we do not think that maturity effects will have undermined the validity of our results. As mentioned previously, several participants reported that their confidence in using the different reporting formats increased as they progressed through the tasks. *Learning effect*, there was not a learning effect in this experiment as there was only one treatment. *Testing effects*, all participants have studied the same material in the familiarisation tutorial session. Very few students have experience with security incident analysis. There was not any cheating because the experiment was on a one-to-one session. *Instrument effects*, the participants were given the same type of tasks and the answers were evaluated by the same marking scheme. Evaluator bias was addressed through the use of two independent security experts during the assessment phase. Evaluators are the colleagues of the author. However, as is mentioned, the group identifiers were removed so that Rater A and B marked the answers without knowing whether or not

the participants had access to the GST diagram. We do not think their relation with the author can bias the results.

5.6.2 External validity

External validity is the possibility to generalise the results beyond the current experiment. We addressed these concerns by selecting a broad cross section of participants including individuals with diverse background to reflect the those of managers and technical staff who must cooperate to implement the recommendations in security incident reports. The participants were undergraduate and postgraduate students. Using students in such experiment is common for practical reasons when the professionals are less available and expensive. However, the generalisation of the results to different target groups needs to be carefully considered. For this reason, Chapter 6 conducts industrial evaluations with healthcare professionals.

It is important to stress that this was a preliminary study. The sample size was relatively small. This was due to practical reasons: (1) the approach is new and people have little experience with security incident analysis; (2) the tasks were complex; (3) participation is voluntary. This also reflects a compromise between the need to study an adequate population of potential end users and the need to conduct a prolonged and detailed analysis of a real case study.

It is difficult to generalise the results to healthcare professionals. However the findings from this experiment provide the basis for future study with industry. Our work did yield important insights into the difficulties that engineers face when trying to understand the implications that previous security incident reports have for their own organisations.

5.7 Conclusions

5.7.1 Findings

An empirical study was conducted to evaluate the usability of the Generic Security Template in terms of accuracy, efficiency, ease of use and task load in assisting the identification of the lessons learned and the security argument on the supportive relationships between the lessons learned and security requirements. The results show that participants will be better able to identify the security issues and recommendations and reasoning about the supportive relationships between the lessons learned and security

requirements with the help of the Generic Security Template than using text-based documents alone. The task load is lower while using both the template and text report than using the text report alone. Moreover, the feedback of the experience with the Generic Security Template shows that it tends to assist the identification of the lessons learned from the security incidents, and make it easier to complete the tasks compared to the text-based approach. People's subjective feedback of the Generic Security Template is positive, which is consistent with the results obtained from quantitative analysis.

A list of suggestion to improve the Generic Security Template had been identified using the Cognitive Dimensions and from the subjective feedback. There are recommendations regarding the visibility of the Generic Security Template, to add colour to the Generic Security Template to improve the visualisation, and decomposition of the lessons learned notation to decompose the complex lessons learned notation that contains more than one learning points and the multi-view design for different target users. We will consider those recommendations in the future design of the Generic Security Template. In particular the use of students is a limitation, healthcare security professionals need to be involved in future validation.

5.7.2 Contributions

A large amount of subjective information was collected in this experiment, including participants' free-text answers about security issues and recommendations, and their subjective feedback on the advantages and disadvantages of the Generic Security Template. The participant's free-text answers enable the researcher to examine further the extent to which the Generic Security Template can help to improve the comprehension of security incidents. This was measured by examining their answers using independent experts. This achieved a higher level of accuracy in measuring the comprehension of graphical models. Moreover, the participants' subjective feedback provided multiple directions for further improvements of the model.

There have been numerous empirical studies to evaluate the utility and usability of graphical notations, including Entity-Relationship diagrams [194], UML [180, 195] etc. However, as far as we are aware, there have been no previous studies to assess the strengths and weaknesses of graphical notations to help understand security incident reports. In this chapter, we have presented the results derived from an initial study into the use of Goal Structuring Notation (GSN) to represent and reason about the recommendations made in a report of a data confidentiality breach involving the

US Veterans' Affairs Administration. We were able to show significant benefits from the use of a graphical technique as well as a textual report in answering a number of questions when compared to the more conventional use of text-based incident reports along. However, we could not demonstrate any significant benefits in terms of the time taken to complete our experimental tasks.

5.8 Summary

This chapter uses one instance of the Generic Security Template to empirically evaluate its usability in assisting the identification of the lessons learned from a security incident in comparison to the traditional freestyle text-based approach. In the next chapter we conduct a study with people working in a healthcare organisation to investigate the organisational context where this approach can be applied and assess industry's acceptance towards this approach.

Chapter 6

Investigation on the Acceptance of the Generic Security Template in Healthcare Systems - An Industrial Evaluation

The Generic Security Template (GST) aims to provide a way to feed back lessons from security incidents to the ISMS. Chapter 5 has evaluated the usability of a GST in assisting the identification of the lessons with university students. The results provide insights into the difficulties that the healthcare professionals have in real practice. In this chapter, we conduct a case study with people working in a Chinese healthcare organisation and assess their acceptance of this approach.

This chapter is divided into the following sections. Section 6.1 introduces the study. Section 6.2 outlines the evaluation plan, including the objectives of the study, target organisation, participants, study materials and pilot test. Section 6.3 introduces the study process. Section 6.4 analyses the results. Section 6.4 discusses the conclusions and contributions. Section 6.5 summarises this chapter.

6.1 Study initiatives

The GST proposed in this thesis has adapted the GSN approach to capture lessons from information security incidents. Since this is the first time to introduce the GST into healthcare organisation, we aim to gain understanding of healthcare professionals' general attitudes towards this new approach to guide further investigation.

A five months internship was accepted in 2013, with a Chinese healthcare organisation, the redacted central hospital, on a newly initiated Security Strengthening Program (SSP). The redacted central hospital started using an electronic healthcare system from 2008 and were looking for recommendations to improve their security system. The internship examined the organisation's information security management system and provided recommendations on improvements. This internship provided the opportunity to obtain more knowledge about information security management in healthcare organisations in China and their support enabled us to evaluate the GST in an organisational context.

6.2 Study design

Pragmatic constraints and ethical concerns over the use of real world case studies limited our ability to conduct large-scale quantitative studies. Security experts within hospitals and medical centres face an increasing array of demands and requests that leaves little opportunity to participate in these studies [74]. We are, therefore, extremely grateful for their participation in the qualitative feedback sessions that are documented in this chapter. There is little previous literature and research on the information security management in Chinese healthcare organisations. This case study allows us to explore an unfamiliar context as the basis for further research [196].

6.2.1 Study objectives

This study aims to find out the general views of GST, from participants with experience of dealing with patient data in hospital. This study involves different occupational communities including physicians, nurses and technicians, as different occupational communities can have different perspectives toward the use of information security technologies in healthcare [74]. Since this is the first time to introduce the GST into a healthcare setting, it is worthwhile to study general attitudes towards this new approach, which forms the basis for future evaluation. The study objectives are to,

- Study current information security management in the host healthcare organisation;
- Study the current mechanisms to feed back lessons from security incidents to ISMS in the host healthcare organisation;

- Study the healthcare and IT professionals' attitudes towards the Generic Security Template.

6.2.2 Target organisation

The research objectives were approached by analysing qualitative data from interview studies of participants from the redacted central hospital in China. The redacted central hospital is a tertiary level hospital in China and has the highest level of maturity in terms of healthcare information systems. They currently use the security standard GB/T22239 (Information security technology - Baseline for classified protection of information system) for information security management. The guidance uses a five level information security classification system. Organisations are required to comply with the GB/T22239, by achieving an appropriate level. For example, the guidance of the health industry information security level protection issued by the Ministry of Health of the Peoples Republic of China requires that health information systems and related units should be self-examined in accordance with GB/T22239 [98]. In particular, the tertiary level hospital needs to achieve at least the third security level characterised in GB/T22239 [106].

6.2.3 Participants

Information sheets were disseminated to each department of the redacted central hospital. The participants attended this study voluntarily. Fifteen were recruited including ten healthcare professionals and five IT professionals working in this hospital. Since the aim of the study is to explore users' experiences of the evaluated approach, rather than generalizing the results, we focused on a small number of participants. This provided suitable coverage of a range of stakeholders across the organisation. The sample was also limited by our desire to conduct detailed and focussed interviews with key individuals in healthcare organisations building on our previous work of an empirical experiment with students.

6.2.4 The study material and pilot test

The study materials include a background questionnaire, interview questions, GST related materials and a post-interview questionnaire (technology acceptance questionnaire). The study design was reviewed by one security expert and one psychology

expert. They helped revise the interview design to make sure the questions addressed the objectives of the study. This study was also pre-tested with two people, one IT professional and one healthcare professional from the redacted central hospital. This is to make sure they can understand the study materials. An important issue identified in the pilot study was to avoid asking sensitive probe questions due to culture issues [197]. Therefore we have to avoid the questions such as “what are the weaknesses of your existing way to learn from security incidents?” The study materials were originally created in English. Prior to being conducted in China, the materials were translated into Chinese. The study conductor is a Chinese native speaker. The translation was reviewed by a second person with a TEM 8 certificate (Test for English Majors Band 8), which is the highest level for English major students [198] to ensure that the translation was precise.

6.3 The study process

6.3.1 The consent form

This experiment adhered to the BPS ethical guidelines, and has been approved by the FIMS ethics committee of the University of Glasgow (ref: CSE01243) (Appendix C.1). The participants completed the consent form before starting the study.

6.3.2 The background questionnaire

Participants were invited to fill in the background questionnaire. This collects the demographic information including job position, gender, education background, years of working experience and experience with security incident handling.

6.3.3 The interview

We conducted semi-structured interviews in this study. The objectives (see section 6.2.1) were transformed into the interview questions (Appendix C.4). There were three main themes within this interview,

The current information security management in the host healthcare organisation.

The participants were asked to describe general security management in the redacted central hospital. We have developed several probe questions as sub-themes for exploration, attached in Appendix C.4. Those sub-themes are based on the existing literature

on management support [199], security culture [200], security awareness [201, 202], and security effectiveness [203]. The information collected under this theme provides a general understanding of the current information security management within the host organisation.

The current mechanisms to feed back lessons from security incidents to ISMS in the host healthcare organisation. The participants were asked to describe their incident handling process, the dissemination of lessons learned and how they feed back the lessons to information security management.

Participants' attitudes towards the Generic Security Template. The participants were presented with a GST as is shown in Figure 6.1, based on the Veterans Affairs incident in the US and the related text based document including an extract of text-based report and the security guidelines FISCAM that are related to this incident. We explained how the GST is created from the text based document. The participants were then invited to comment on whether the GST is useful to feedback the lessons learned to ISMS comparing to the existing methods.

We were not allowed to record the conversation due to the sensitivity of the research themes. Therefore, we took field notes during the interview. After the study, a summary based on the field notes was generated and sent to the informants for confirmation and acceptance within one hour. This is to validate that the information is accurate and complete. All confirmations were returned by the participants.

6.3.4 Post-interview questionnaire

A number of models had been developed to evaluate the acceptance of technologies. Those models originated from different theoretical disciplines such as psychology, sociology and information systems. These technology acceptance models include theory of reasoned action (TRA) [204], technology acceptance model (TAM) [205], motivational model [206], theory of planned behaviour (TPB) [207], combined theory of planned behaviour/technology acceptance model [208], model of personal computer (PC) utilisation [209], innovation diffusion theory [210], and social cognitive theory [211]. Venkatesh proposed a new IT acceptance and use model, the unified theory of acceptance and use of technology (UTAUT) [212], which aimed to unify eight prominent competing IT acceptance and use models [212]. The authors contend that the new model successfully integrates all constructs in previous models and can explain variance in IT behavioural intention and use better than the previous models. It was able to

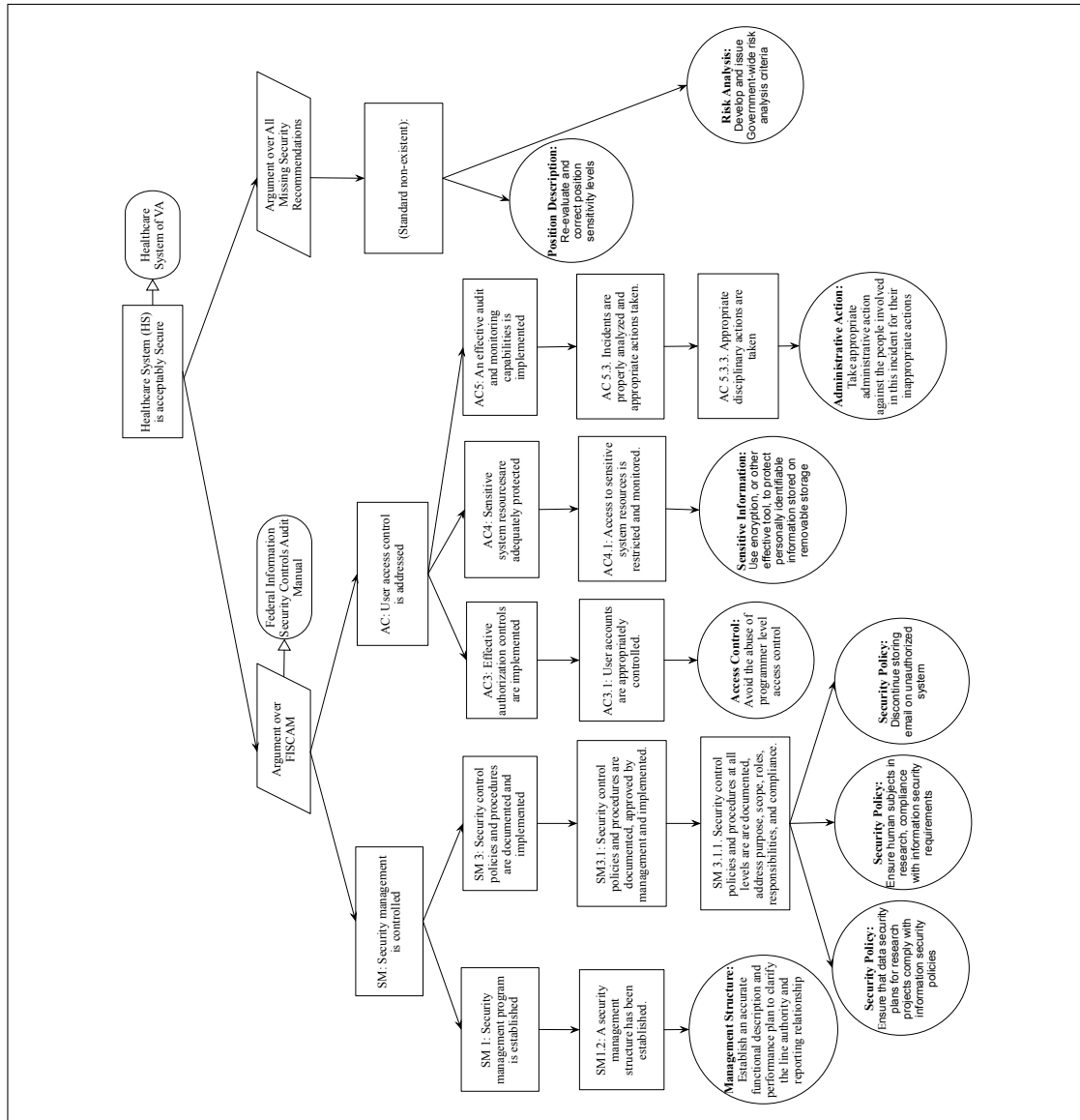


Figure 6.1: An example instance of the Generic Security Template - VA 2007 data leakage incident

explain 69% of intention to use IT (technology acceptance) while other previous models explained approximately 40% of technology acceptance [212]. In this dissertation we adapt the UTAUT model to explore participants' attitude toward our approach. The finalised questionnaire is attached in Appendix C.5.

6.4 Results of the study

This section presents the major themes in the data. The findings are grouped according to the research objectives. The data was further cross-referenced with the collected document for triangulation [213].

6.4.1 Background questionnaire

The healthcare professionals who participated in this study, included four doctors (males) and six nurses (females). Five IT professionals participated in this study, four of them are IT engineers (one female and three males) and one of them is an IT manager (male). The educational background ranges from honoured bachelors to masters. All of the IT engineers have experience with security incident handling. Among the healthcare professional, two nurses and one doctor have been involved in the security incident handling process, the rest of them have no experience with information security incident. Their background information is summarised in Appendix C.6.

6.4.2 Information security management

The participants were asked to describe the general security management system in terms of management support, security culture, security awareness, and security effectiveness. The information collected was to gain a general understanding of information security management within the host organisation.

Management support. Management support is a critical information security component to protect information assets [214]. In general, the management team supports information security practices within the organisation. They have designed the employee entrance security training program. The organisation has also initiated the security improvement program and on-going Security Strengthening Program (SSP). However, it does not seem to be a priority of the management. As is stated by one of the healthcare professionals, “the management rarely talks about security unless serious incidents happen” and “they seem to care less about security, unless there is

something starting to affect the business function”. One of the IT professions said “the management focuses more on the business function of the healthcare information systems, compared to security”.

Security awareness. User awareness, education, and training are critical information security components [214, 215]. Timeliness and consistency of security information are the key factors of a security awareness program as the security risks profiles are changing all the time [216]. The organisation provides security training to new employees, but there is no on-going training to refresh their information security knowledge. Employees are not provided with accessible information security material to update their knowledge probably because information security is not a priority for healthcare professionals [74]. However, the healthcare professionals do demonstrate some basic understanding of information security. For example, an IT professional stated “we were warned of the consequences caused by accessing unauthorised patient records”, “We are not allowed to reveal patients’ information outside the working place or to irrelevant people”. The organisation is said to have other ways to increase staff awareness by informing them of ways to avoid recent security incidents by phone calls or through informal meetings. Comparing to the healthcare professionals, the IT professionals are provided with more comprehensive training on security related techniques and they are encouraged to get professional qualifications.

Security culture. Winkel defines security culture as the system of collective moral concepts, mindsets and behaviour patterns anchored in the self-conception of a social unit and instructing its members in dealing with security threats [217, 218]. Appropriate and effective information security management implementation requires a combination of favorable organisational culture traits such as involvement, consistency, adaptability, and sense of mission [219, 220]. The organisation values the importance of security and their management and colleagues were said to be concerned with security. The management has initiated the security improvement program and on-going Security Strengthening Program (SSP). The organisation has a stated aim of achieving a secure operation by following the security standards [98]. In addition, employees violating the security standards will be punished. However, they arguably do not have activities to promote good security practices such as reward staff for good security behaviour [221, 222].

Security effectiveness. Security effectiveness refers to the ability of IS security measures to protect against the unauthorised and deliberate misuse of assets of the local organisational information system by individuals, including violations against

hardware, programs, data, and computer service [223]. Previous researches show that it is affected positively by management support and security culture [217, 220]. The IT manager stated that the organisation had achieved most of their security goals as the system is maintained strictly by following the security standards. The healthcare professionals also found their security management effective, as they stated “the organisation has taken security controls such as firewalls and anti-virus software to protect the system, and they regularly updates system patches”.

6.4.3 Security incident learning

As opposed to separated responsibilities [6, 36] in handling security incidents and general incidents, the redacted organisation has only one team, the IT department, responsible for handling all incidents. The IT department treats security incidents equally as general incidents. When a security incident happen, it is logged through phone calls to the security team. The severity level of the security incident is then decided according to the severity level defined by the organisation. The hospital does not have an electronic incident logging system to manage incidents, and the work is all paper based. Low level security incidents refer to those that affect only a small part of internal systems, and do not have a direct impact on patients, e.g. if there is only one end user computer down. A security engineer was then assigned to the incident till the incident is solved or mitigated. High severity incidents refer to those that are critical to the systems’ ability to function, with high level of risk, and impacts on patients, such as the crashing of a critical business function. The incident response team will be formed including the IT manager and all the other IT professionals and the people involved in this incident. A post-incident review will then follow. Informal meetings will be held to disseminate the learning from incidents to different stakeholders. As we can see, although they do not have an electronic incident management system, they have a relatively complete process to deal with incidents including preparation, incident investigation, incident mitigation, post-incident learning, an incident response team [36] as well as clear rules of incident response according to the severity level. This demonstrates a level of maturity for incident management. However, we have identified the following problems of the security incident handling process, especially in the communication of lessons learned to the ISMS of the host organisation.

Incident response and knowledge gathering. The handling of low level security incidents focuses more on technical aspects to recover business functions, and places

less emphasis on knowledge gathering of the lessons learned from those incidents. The IT manager stated “the business function is the most important, everyone must prioritise it, to turn the system back to normal”. At the same time the team gathered security knowledge to solve the issues throughout the incident handling process, which are crucial for future learning. However, this information was either not documented or partly documented, which makes it difficult to share with others. The handling of high severity incidents is more comprehensive. A security incident team is formed to investigate the incident. Lessons are documented and there is a post-incident report generated after the incident, including business impact, in-depth causal analysis and remedial actions. These are similar to the existing publicised data incident reports [14, 15]. However, the hospital’s post-incident reports are for administrative purposes to show that the incident has been dealt with. Those report were rarely viewed by others, resulting in limited knowledge to be shared from the incident handling process.

Information dissemination. For low severity incidents, the knowledge obtained from the incident handling process was either not documented or documented in pieces. There has not been a systematic way to document and manage learning, hence created difficulties in disseminating this knowledge. For high severity incidents, there is information disseminated through phone calls and informal meetings, however, people outside the incident response team complained about the lack of incident knowledge being distributed. A more detailed post-incident report is produced for high severity incidents, however, it is hardly accessible by people outside the incident management team. Even though the post-incident reports can be made available, employees who have seen the reports find it difficult to digest as it contains comprehensive inter-related information. As is stated by a healthcare professional who had involved in the incident handling process, “the document is so difficult to read, and everything is mixed together”. This is probably because the post-incident report is written for an administrative purpose rather than an engineering purpose [45]. This finding is consistent with Ahmad’s study with a financial organisation [6]. There is a need for the conversion of the post-incident report into a learning document, that is easily understood by many in the organisation.

Lessons learned to feed into the ISMS. For low severity incidents, the focus is on solving the direct causes. For example, the IT professionals stated “we focus on solving the problem directly and until it is back to normal”. However, the aim of the incident analysis is to identify root causes, which is often a security management issue (e.g. not having a policy for configuring firewalls) rather than a technical prob-

lem (e.g. firewall not properly configured) [5, 6]. An IT professional's feedback well supported this opinion, "the real causes might be in the security procedure itself, that a procedure makes people to cause error". For high severity incidents, the detailed post-incident reports were generated. However, when examining the contents of the report, we found that they have not stated clearly whether the incident is caused by inappropriate implementation of policies/guidelines/standards, or the lack of relevant policies/guidelines/standards, or whether the lessons learned had led to the revision of policies/guidelines/standards. However, the whole incident handling process seems to lack of a mechanism to communicate learning of lessons within the security information management procedures. There is a need to investigate why a potential incident is not adequately covered by the policies/guidelines/standards, that may lead to further improvement of policies/guidelines/standards and may prevent future incidents.

6.4.4 Attitude towards the Generic Security Template

The participants were presented with a GST instance as shown in Figure 6.1. We explained how the GST instance was created from text-based security incident reports. The participants were then invited to comment on the GST. The IT professionals and healthcare professionals have demonstrated different perspectives towards the use of the GST. According to Orlikowski and Gash [218], various organisational stakeholders interpreted technology differently. An understanding of people's interpretations of a technology is critical to understand their acceptance towards it. They proposed the technological frames to analyse different stakeholder's interpretations towards a technology [218],

- *Nature of Technology*, refers to people's images of the technology and their understanding of its capabilities and functionalities.
- *Technology Strategy*, refers to people's views of why their organisation acquired and implemented the technology. It includes their understanding of the motivation or vision behind the adoption decision, and its likely value to the organisation.
- *Technology-in-Use*, refers to people's understanding of how the technology will be used on a day-to-day basis, and the likely or actual conditions and consequences associated with such use.

We adopt Orlikowski and Gash's technological frames to analyse the results.

6.4.4.1 Healthcare professionals' attitude

Nature of Technology

The healthcare professionals demonstrated a basic understanding of the GST. They considered it to be “some way similar to the communication of security incidents in the department meeting”. They have identified the benefits of the GST in communicating the security incidents. A healthcare professional said, “it makes things clearer, breakdown issue into details”, “we can easily focus on a specific issue they (IT professional) talk about ”.

Technology Strategy

The healthcare professional believed that the use of the GST is to formalise the way to communicate the security incidents, as compared to their old way that uses free style presentations in the meeting. As is stated by one of the healthcare professionals, “previously, different IT professionals present security incidents using different ways of their own, but I like this structured way, that makes everything easy to follow”.

However, there were also concerns raised about the necessity to adopt the GST. As is stated by a healthcare professional, “I am not sure if it is necessary to make the changes, as we rarely communicate incidents unless after a severe security incident”.

Technology-in-Use

The healthcare professional have some difficulties in understanding some technical terms in this GST instance. As is stated by a healthcare professional, “if you don't explain the concept ‘access control’, I could not understand it by myself”. They suggest either a document providing definition for technical terms or the IT professionals' assistance is needed to help them. They also complained about the “lack of multi-view design” of the GST. As is stated by a healthcare professional, “‘access control’ seems to be IT professionals' responsibility”.

6.4.4.2 IT professionals' attitude

Nature of Technology

Similar to the healthcare professionals, the IT professionals also find the GST to be effective in communicating security incidents. An IT professional stated that, “this will be especially helpful to discuss security issues; easier to navigate between different notations”. The IT manager stated “it brings together everything that involves different

stakeholders; it can facilitate decision making and balance the interests of different stakeholders in a discussion”.

Compared to the healthcare professionals, the IT professionals demonstrated a deeper understanding of the GST in terms of its capabilities and functionalities. They believe that it is a good way to inform the implementation of security standards. An IT professional stated “it provides a process to track what goes wrong at which level in the security standards that causes the incident”. “It can let us know how well we have implemented the security standards and which part needs to be improved”. Moreover, they have found the lessons which cannot be mapped to any security requirements especially helpful. One IT professional said, “this will help us identify a new security requirement that was not considered by the standard or organisation ”.

However, they raised concerns about the GST on the ambiguity of the relationships between the lessons learned and the security standards. As is commented by one of the IT professionals, the GST does not suggest clearly about the relationships between lessons learned and the security requirements of the security standards, and there are no formal rules to guide the mapping. An IT professional said “it will be good to have some general rules to follow for the mapping”. This is due to the subjective nature of the GSN, which the GST is based upon, that leaves the security arguments open for review [7]. The IT manager gave additional comments on the lessons learned that do not map to any security requirement. He suggested that those lessons should be aligned with the existing security standards, rather than being grouped as “Standard non-existent”. He suggested to move the lessons “Risk Analysis: Develop and issue Government-wide risk analysis criteria” to be under the security requirement “SM2.1: Risk assessments and supporting activities are systematically conducted”, and the “Position Description: re-evaluate and correct position sensitivity levels” to be under the security requirement “SM1.3: Information security responsibilities are clearly assigned”, as is shown in Figure 6.2, indicating those lessons might be the missing aspects of existing security requirements. He justified this change as a step forward to “track which security requirement requires an update as are informed by those lessons”.

Technology Strategy

The IT professionals believe that, the use of the GST tends to change the way to report and communicate the security incidents. They mentioned that, presenting lessons from security incidents in this way “forces us to identify the root causes, which is al-

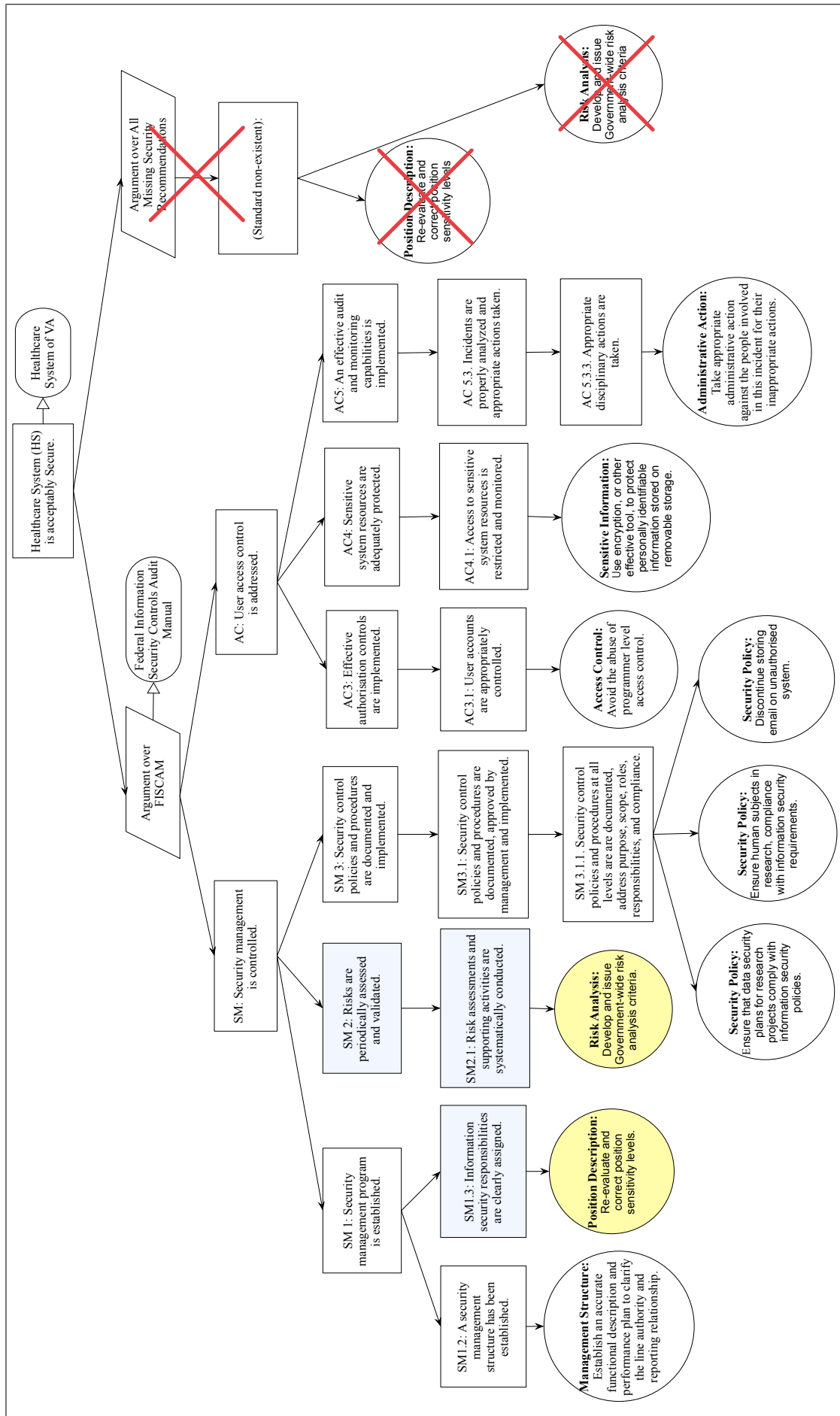


Figure 6.2: Customised instance of the Generic Security Template - VA 2007 data leakage incident

ways inappropriate implementation of a standard, rather than simply dealing with the direct causes in the incident handling process”. This is consistent with our previous finding that their current security incident handling focuses on solving the direct causes rather than look into the procedure that makes people to cause error. They also identified the GST’s role as “bringing together pieces of notes generated in the security incident handling process, and easier to track previous lessons”.

Technology-in-Use

To use the GST, the IT professionals are required to learn a new technique to report the security incidents. One of the IT professionals complained “I cannot predict how effective it will be, and how worth the effort is”. From a long term perspective, the IT professionals tend to agree that “the benefits might outweigh the efforts once everyone starts getting used to this new technique”. This is consistent with the findings in safety area, where GSN has been widely adopted. The proponents of GSN argue that its expressive power is well worth the extra learning time and there is positive indication that the use of the GSN is cost effective [169].

They were also concerned about scalability issue of the GST with the expansion in everyday use, “the template could become unmanageable if it documents a complex incident or it is an integration of many tiny incidents”. This issue can be addressed by borrowing the experience from the use of GSN in safety area, to break the template into sub-cases. For even more complex cases, experience on GSN modular development can be borrowed from safety area [47]. The experience in safety area has been proved to be successful in solving similar issues [47]. However, whether it can be effective in our scenerio requires further examination.

As we could see that IT professionals and healthcare professionals have different interpretation of the GST. They have made the judgments based on their own knowledge, experience and work style. To the healthcare professionals, the GST serves as a tool to communicate security incidents, however, they do not see this tool as a must that the organisation has to implement, as they do not frequently use it in their everyday work, and they doubt about the efforts to learn and adopt such a new technique. In comparison, the IT professionals identified the advantage in utilizing the security lessons to inform the implementation of the security standards. Although the engineers have to learn a new technique, they still think the long term benefits gained is worthwhile the effort.

6.4.5 Strengths and weaknesses

Based on the analysis above, the strengths and weaknesses are summarised in Table 6.1 and 6.2,

Table 6.1: The strengths of the Generic Security Template

The Strengths	Healthcare Professionals	IT Professionals
An effective way to communicate lessons learned	... especially helpful to discuss security issues; ... easier to navigate between different notations; ... brings together everything that involves different stakeholders; ... facilitate the decision making and balance the interests of different stakeholders in a discussion.	... this will be especially helpful to discuss security issues; ... easier to navigate between different notations; ... it brings together everything that involves different stakeholders; ... it can facilitate the decision making and balance the interests of different stakeholders in a discussion.
A formalised way to communicate lessons learned	... previously, different IT professional presents security incident using different ways of their own, but I like this structured way, that makes everything easy to follow.	
A way to inform implementation of security standard		... a process to track what goes wrong at which level in the security standards that causes the incident; ... let us know how well we have implemented the security standards and which part needs to be improved; ... this will help us identify a new security requirement that was not considered by the standard or organisation.

Table 6.2: The weaknesses of the Generic Security Template

The Weaknesses	Healthcare Professionals	IT Professionals
Extra efforts to learn a technique	... not sure if it is necessary to make the changes, as we rarely communicate incidents unless after a severe security incident.	... cannot predict how effective it will be, and how worth the effort is.
Scalability issue of the GST		... template could become unmanageable if it documents a complex incident or it is an integration of many tiny incidents.
Comprehension of the GST	... if you don't explain the concept 'access control', I could not understand it by myself.	
Ambiguity of mapping between lessons learned and the security standards		... it will be good to have some general rules to follow for the mapping; ... track which security requirements require an update as are informed by those lessons.
Multi-view design	... lack of multi-view design; ... 'access control' seems to be IT professional's responsibility.	

6.4.6 Senarios identified to apply the Generic Security Template

Opinion was generated about the use of the GST. The healthcare professionals and IT professionals who support the use of the GST help to identify the following scenarios where it can be applied in,

Scenario: communicate security incidents in department meeting. The healthcare professionals have found it useful in communicating lessons learned from security incident, and suggest adopting this method for demonstrating security incidents in the department meeting in future.

Scenario: inform the implementation of security standard. The IT professionals have found it useful in informing the implementation of the security standards. This identifies future work to focus on how the GST can be used to inform the implementation of standards.

6.4.7 Acceptability questionnaire results

6.4.7.1 Acceptability of the healthcare professionals

Figure 6.3 presents the healthcare professionals' attitudes towards the acceptability of the GST. In general, half of the healthcare professionals are satisfied with the GST. Four out of ten of them are neutral and one disagreed with it. Eight of the healthcare professionals agreed that the GST can enhance the effectiveness to communicate lessons learned. One healthcare professional provided very negative feedback. Over half of the healthcare professionals agreed that the tool is easier to use and interaction with the tool is clear and understandable. Two out of ten of the healthcare professionals disagree. Around half of the healthcare professional expressed their willingness to use it given the resources and tool available. Others who disagreed had concerns over the technical terms that are difficult to understand. Only two of the healthcare professionals found it fit into their work style. This might be due to their resistance towards new technology especially when they have little experience of information security, as well as the lower frequencies that the GST is likely to be used in their everyday practice. This result is consistent with the finding from the analysis in section 6.4.4.1.

6.4.7.2 Acceptability of the IT professionals

The IT professionals are generally satisfied with the overall experience of the GST. A significant difference is, four out of five of the IT professionals find it fit into their

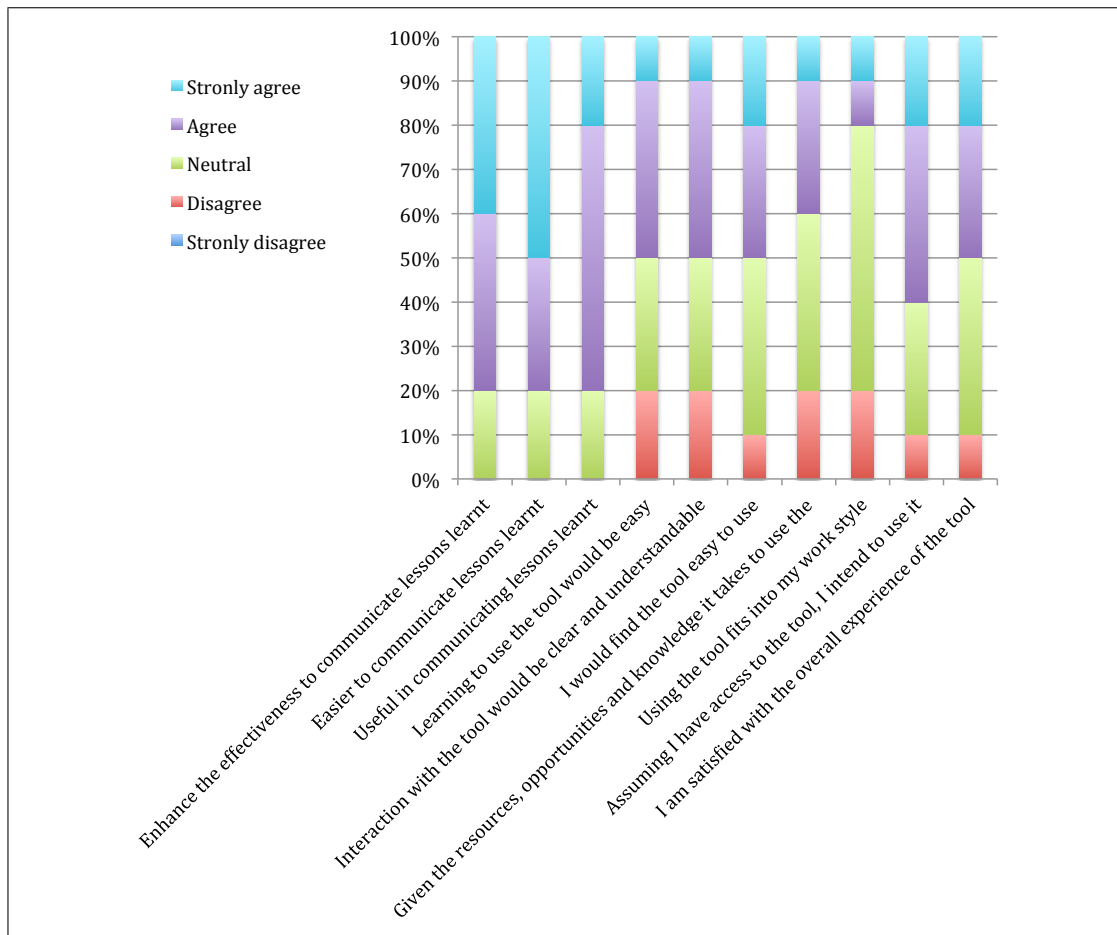


Figure 6.3: Healthcare professionals' attitude towards the acceptability of the GST

work style, compared to the healthcare professionals, that two out of ten of them find it fit into their work style. This is probably because security is not the healthcare professional's priority in everyday work. In comparison, the IT professionals' experience with information security, allows them to identify the potential benefits of the GST, thus they demonstrated more interests toward the GST. One security expert felt it would be hard to learn to use the tool. He raised a concern about the creation of the GST as mentioned earlier "I cannot predict how effective it will be, and how worth the effort is". This result is consistent with the finding from the analysis in section 6.4.4.2.

6.5 Discussion

A case study with a representative healthcare organisation in China shows that security management is important to the managers and they are willing to improve their current situation through some initiatives such as the on-going Security Strengthening Pro-

gram (SSP), however, it is not a priority compared to the systems business functions. Their healthcare professionals have taken only the entrance security training, however they demonstrated a basic understanding of information security. The IT professionals have a deeper understanding of security through obtaining professional trainings. The organisation has a stated aim of achieving a secure operation by following the security standards. According to the IT team, they have established security controls according to the security standards and the staff found them to be effective.

Based on the analysis in previous sections, the organisation has a relatively mature incident handling procedure including the definition of different incident severity levels and incident response teams. Learning from security incidents can help avoid serious incidents [39] and should ideally improve information security procedures [6], however, it is not effectively informing improvements of the ISMS in the redacted healthcare organisation. We have identified weaknesses in the handling of both low-level and high-level incidents: (1) for low-level incidents, they lack of a formal way to generate knowledge. They mainly focus on solving issues to recover the system. There is little in-depth analysis of the causal factor that may lead to a procedure issue rather than a technical concern. (2) For high-level issues, they document the business impact, and remedial recommendations, etc. However, the post-incident reports, are for administration only and do not consider the improvements of security procedures. Moreover, knowledge in the form of a post-incident report is usually presented as a lengthy free-text report. Previous chapters and researches have argued text does not alone facilitate the communication of security lessons. GST can be used to effectively communication lessons learned to inform the improvement of security management procedures.

IT professionals and healthcare professionals have demonstrated different attitudes towards the acceptance of the GST. The healthcare professionals considered the GST as a tool to communicate security incidents only and they do not see this tool as a must as they do not think it fit into their work style [74]. In comparison, the IT professionals identified the advantage in utilizing the security lessons to inform the implementation of the security standards. The people who support the approach identified scenarios for communicating security incidents and informing the implementation of security management standards.

The IT professionals raised concerns about the GST on the ambiguity of the relationships between the lessons learned and the security standards and suggested to develop rules to guide the mapping. In particular, the IT manager suggested that the

security lessons should be aligned with the existing security standards indicating they might be some missing aspects of existing requirements. The IT manager customised the example case as is shown in Figure 6.3 and justified the change as a step forward to track which security requirement requires an update as are informed by those lessons. This is not the first time the mapping was challenged in this research. Recall Chapter 4, where we identified the difficulties when the lessons learned were found to be related to more than one security requirements. We accepted this change because the IT manager raised this request and he is the person who can make the final decision whenever a new IT technology is introduced into the organisation. We have developed new guidance for mapping, as is shown below, to overcome this problem in Chapter 4,

Starting from the bottom-level goals in the goal structure, if a lesson learned is related exclusively to a bottom-level goal, it should be mapped to this bottom-level goal. If a lesson learned is related to more than one bottom-level goals in the goal structure, this lesson learned should be mapped to the nearest parent goal where those bottom-level goals share the same parent goal (Chapter 4).

By considering the suggestions from the IT manager, we improve the guidance about the mapping between the lessons learned and the security standards. Depending on their relationships with the goals, those lessons learned have been divided into four types,

Starting from the bottom-level goals in the goal structure, (Type I) if a lesson learned is related exclusively to a bottom-level goal, it is defined as Type I. Then this lesson learned should be mapped to this bottom-level goal. (Type II) If a lesson learned is related to more than one bottom-level goals in the goal structure, it is defined as Type II. Then this lesson learned should be mapped to the nearest parent goal where those bottom-level goals share the same parent goal. (Type III) If a lesson learned is related to none of the bottom-level goal, go up to check other goals, check and decide whether it is related to a higher level goal in the structure. If yes, it is defined as Type III, this lesson learned should be mapped to this related goal. This indicates a probably missing aspect of a higher level goal. (Type IV) If a lesson learned is related to none of the goals in the goal structure, it is defined as Type IV, then a new goal named “(Standard non-existent)” should be created to link this lessons learned to the top goal. This indicates a missing aspect of the whole security management guidelines or standards.

The customised instance of the GST was used to exemplify the application of the new guidance. After adding the lessons learned types, Figure 6.2 changes to be Figure 6.4.

Type I

Lesson learned

Sensitive Information: Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage.

Security requirement bottom level

AC 4.1: Access to sensitive system resources is restricted and monitored.

Decision on lesson learned type

The lesson learned is found to be exclusively related to bottom level goal AC 4.1.; therefore, it is a Type I lesson learned.

Type II

Lesson learned

Access Control: Avoid the abuse of programmer level access control.

Security requirement bottom level

AC-3.1.1. Resource owners have identified authorised users and the access they are authorized to have.

AC-3.1.2. Security administration personnel set parameters of security software to provide access as authorised and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs. (Standard naming conventions are essential to ensure effective configuration management identification and control of production files and programs vs. test files and programs)

AC-3.1.3. Security managers review access authorizations and discuss any questionable authorizations with resource owners.

AC-3.1.4. All changes to security access authorizations are automatically logged and periodically reviewed by management independent of the security function; un-

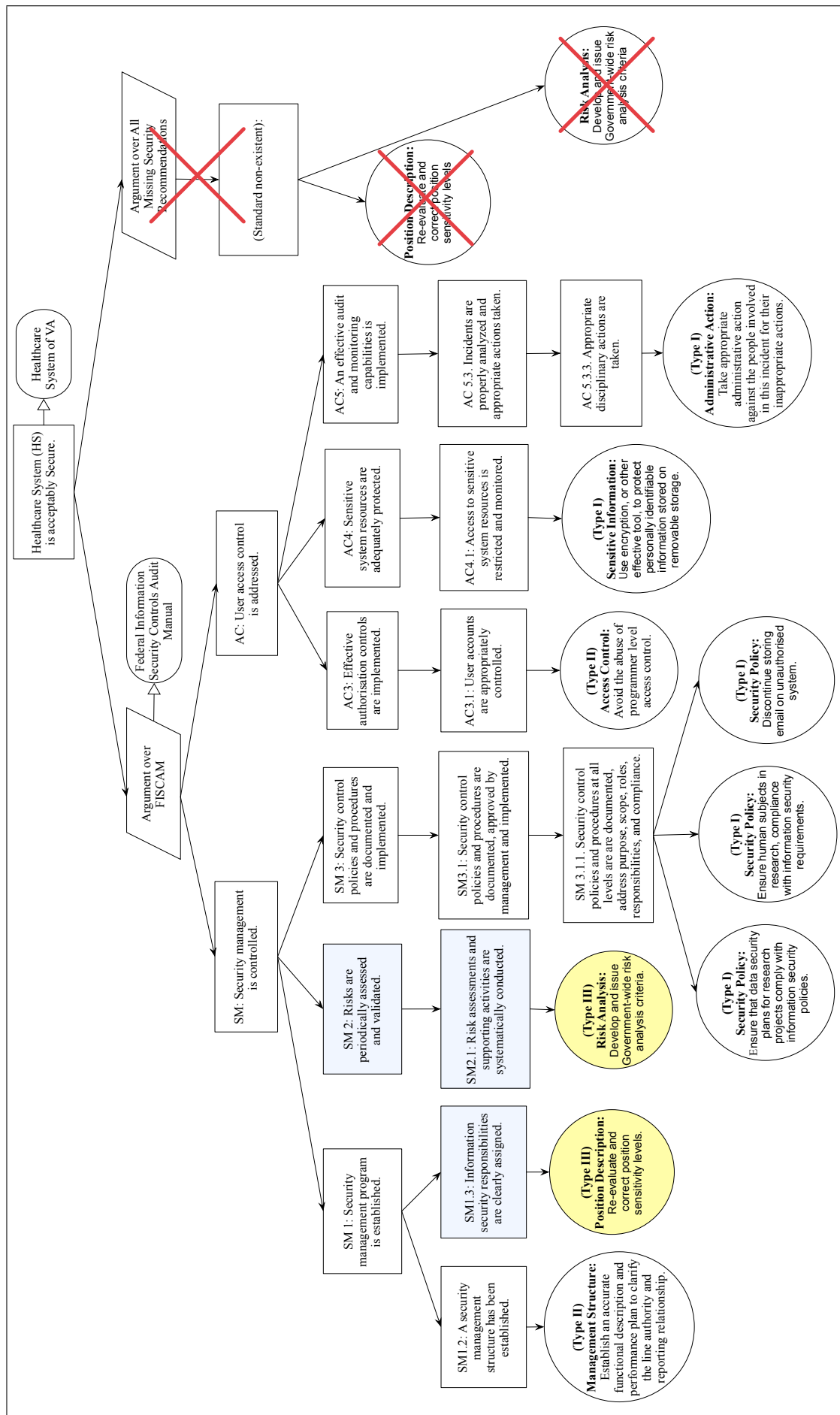


Figure 6.4: Customised instance of the Generic Security Template with lessons learned types - VA 2007 data leakage incident

usual activity is investigated.

.....

Security requirement bottom level - 1

AC-3.1. User accounts are appropriately controlled.

Decision on lessons learned type

The lesson learned is found to be related to more than one bottom-level goals AC-3.1.1 and AC-3.1.2, then it is a Type II lesson learned. This lesson learned should be mapped to the nearest parent goal where those those bottom-level goal share the same parent goal, which is AC-3.1.

Type III

Lesson learned

Position Description: Re-evaluate and correct position sensitivity levels.

Security requirement bottom level

.....

SM-1.3.1. The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviours are clearly defined at the entity wide, system, and application levels for (1) information resource owners and users, (2) information technology management and staff, (3) senior management, and (4) security administrators.

Security requirement bottom level - 1

SM 1.3: Information security responsibilities are clearly assigned.

Decision on lessons learned type

The lesson learned was found to be related to none of the bottom-level goal, e.g. SM 1.3.1....., but it is found to be related to a higher level goal SM 1.3 in the structure. This lesson learned should be mapped to SM 1.3. Therefore, it is a Type III lesson learned. It indicates this lesson is probabaly missing from the goal SM 1.3.

6.6 Summary

This chapter conducted a healthcare evaluation to find out general views on GST from people having experience dealing with patient data. They have provided valuable feedback on the improvements of the GST. In particular, we have accepted the IT professionals' feedback and revise the guidance on mapping between the lessons learned and security requirements. However, the validity of the improvement needs to be evaluated in real practice. Chapter 7 further evaluates the GST with university students to study whether they can use the improved Generic Security Template to structure the insights derived from specific security incident.

The findings from this study are subjective impressions and may not provide direct evidence to show that the organisation can adopt GST. However, the interviews with healthcare professionals in China provided very important insights into the application of our approach. This provides the directions for future work; to gather more direct evidence about whether or not security lessons can be transferred using the Generic Security Template between healthcare organisations in different countries. Moreover, two application scenarios are identified, (1) communicating security incidents in team meetings and (2) informing improvements of the security standard. (1) is similar to the demonstration of the GST in this pre-interview tutorial. Future work needs to expand on (2) by conducting an in-depth study to find out how the lessons learned can be fed back to improve the implementation of the security standards using the GST. In Chapter 8, we use security incidents in different countries, to discover how lessons can be transferred to the redacted central hospital to inform improvements of security management.

Chapter 7

Application of the Generic Security Template to structure a GST Instance from a Specific Security Incident - An Empirical Evaluation

The Generic Security Template has been improved after a series of evaluations. This chapter evaluates the improved Generic Security Template by investigating whether a larger number of students with a computer science background can use the Generic Security Template to structure the insights derived from specific security incident.

This chapter is divided into the following sections. Section 7.1 introduces the objectives of the study. Section 7.2 outlines the study design including the participants, study material, and pilot test. Section 7.3 introduces the study execution. Section 7.4 analyses the results. Section 7.5 discusses the findings, and limitations of the experiment. Section 7.6 summarises this chapter.

7.1 Study objectives

The Generic Security Template has been improved after a series of evaluations. This study aims to find out whether users can apply the improved Generic Security Template to structure the insights derived from specific security incident. In Chapter 4, we have demonstrated that the Generic Security Template can be used to structure the security lessons from real world security incidents happened in US, UK and China. This study generalises the use of the GTS to a large user group. The study objectives are outlined

below,

- Investigate whether users can apply the improved Generic Security Template to structure the insights derived from specific security incident.
- Study whether there is any difference in the performance, efficiency, task load, and ease of use to complete the task between the users with an information security background and users without an information security background.

7.2 Study design

7.2.1 Participants

The security diagrams that provide an overview of the lessons from specific incidents, illustrated for the security incidents, are intended to be accessible to a wide range of healthcare professionals. In contrast, the Generic Security Template is intended to be used by security professionals to structure these specific security diagrams. Pragmatic reasons motivate the use of computing science students in the initial pilot study. We were also concerned to determine whether these techniques could support the exchange of lessons across national boundaries. This study focused on the use of Generic Security Templates in China. We, therefore, recruited 81 participants in Guangzhou. Information sheets were distributed in the computing science department in a university in Guangzhou and 81 university students participated in this study voluntarily.

7.2.2 Study material

Training material. The participants were given a written instruction document (Appendix D.1). The instruction is self-descriptive and twelve A4 pages long. It is the only resource for the participants to obtain training on the use of GST. This instruction introduces, (1) The basic knowledge of GST notations, which includes goals, strategies, context and lessons learned; (2) The steps on how to create the instance of the GST. The creation steps have included the improvement suggestions from previous chapters such as the guidance on deciding the relationships between lessons learned and security requirements; and (3) A small, simplified case study to illustrate the four steps to create an instance of the Generic Security Template.

Task related material. The participants were provided with, (1) a data breach document stemming from the disposal of confidential information, and (2) a guidance on

properly disposing confidential information. Their task was to create an instance of the GST using (1) and (2) by following the instructions in the training material.

Post-study questionnaire. A post-study questionnaire is designed to collect the participants' background information, difficulties encountered in the study, task load and the ease of use of this approach.

7.2.3 Pilot study

A pilot test was conducted with two security experts before the large scale study. The aim was to clarify the training material, task related material and post-study questionnaire. We revised those materials based on the feedback from the first pilot study. A second test was then conducted with two different participants to ensure that these revisions had addressed the initial concerns with the experimental task.

7.3 Study execution

There is often a compromise to be made between controlling experimental variables and ecological validity. Security incidents, typically, involve a number of technical, human and organisational factors. They take time and effort to understand. For this reason, we encourage the participants to take the materials (Appendix D.1) away and only submit their findings when they are happy with the results. This creates the opportunity for collusion, however the analysis was not assessed and the participants were asked to work independently.

7.4 Result analysis

7.4.1 Background questionnaire

Among the 81 participants, 41 of them had previous training in information security and 40 of them had not. They have all attended a talk on the use of the Goal Structuring Notations (GSN). They all have experience with at least one diagrammatic approach such as Entity-Relationship diagram and Unified Modelling Language. Six of them did not return their work. We have removed those incomplete results. Finally we got 75 valid responses, including 38 from the security group and 37 from the non-security group. In the security group, there are 5 females versus 33 males, 4 undergraduate

student versus 36 graduate student. In the non-security group, there are 8 females verses 29 males, 11 undergraduate student verses 26 graduate student.

7.4.2 Measurement of the results

The participants followed the instruction to apply the Generic Security Template to structure lessons learned from an incident. There are four steps and the results are measured within different steps,

In Step 1, the participants are required to prepare the goal structure, which includes the top goal and the rest of the goal structure. Recall Step 1 (Chapter 3 Section 3.3.3.1), the process of identifying the goal structure uses security requirements within applicable standards and guidelines. In this study, we have provided them with a structured text description of guidelines. The aim of this step is to find out whether they can place the structured text description of guidelines into the right syntactic shapes and the right location in the diagram. More details can be found in the task description in Appendix D.3. The participants are given a score for each correct goal. A correct goal must satisfy the criteria (1) the right syntactic shape (squares for goals) (2) the right content, and (3) the right location in the diagram. Figure 7.1 provides an example of the correct goal structure. A score is not given for a goal that violates any of the above criteria.

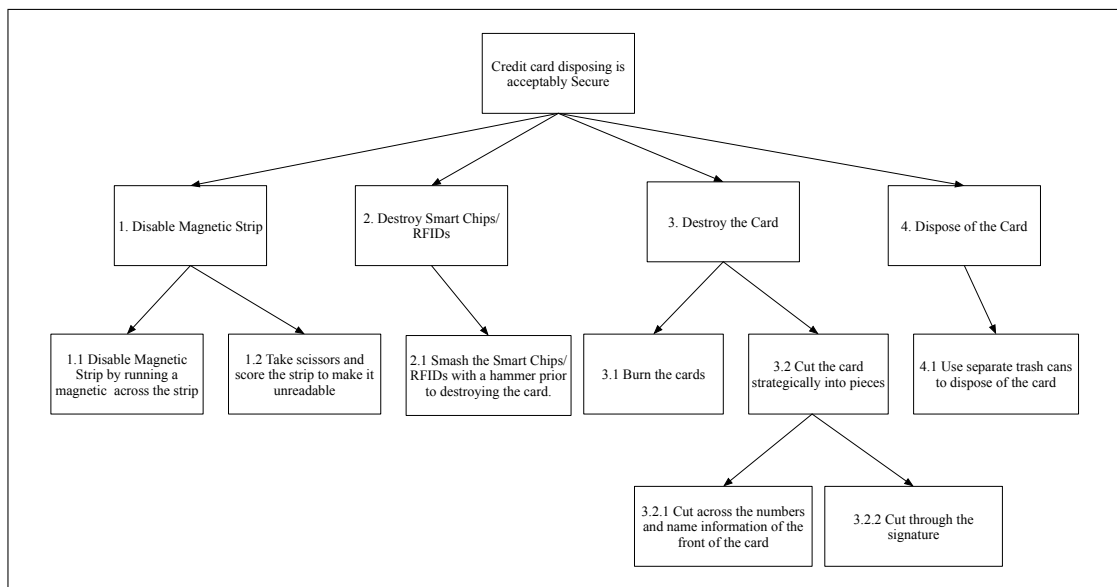


Figure 7.1: Goal structure of the Credit Card Disposing Case

In Step 2, the participants are required to prepare lessons learned. Recall Step 2 (Chapter 3 Section 3.3.3.2), the process of identifying lessons learned required the

analyst to identify key learning points. We have simplified this process by providing a list of learning points in a structured manner. The aim of this step is to find out whether they can place the structured text description of guidelines into the right syntactic shapes. More details can be found in the experiment task description. The participants are given a score for each correct lesson learned. A correct lesson learned must satisfy (1) the right syntactic shape (circles for lessons learned) (2) the right content, and (3) be placed in an appropriate location in the diagram. Figure 7.2 provides an example answer for the correct lessons learned identified. A score is not given for a lesson learned that violates any of the above criteria.

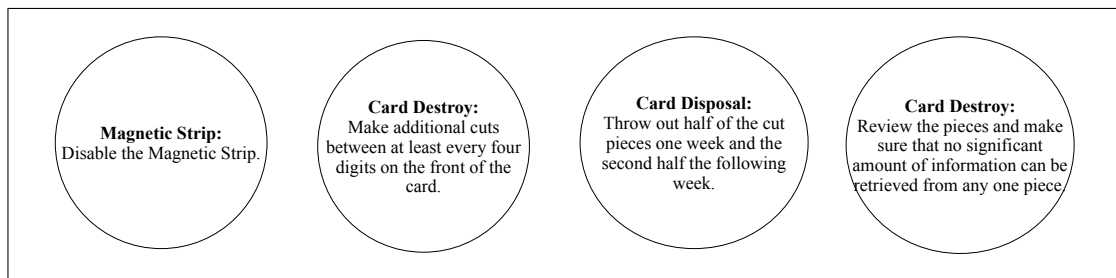


Figure 7.2: Lessons learned of the Credit Card Disposing Case

In Step 3 (Chapter 3 Section 3.3.3.3), the participants are required to map the lessons prepared in Step 2 to the goal structure prepared in Step 1. We have demonstrated and exemplified the rules of mapping (Chapter 6 Section 6.5) in the instruction. The participants are given a score for each correct mapping. A correct mapping must satisfy (1) the right lesson learned type, (2) the right mapping. Figure 7.3 provides an example answer for the correct mapping. A score is not given for a mapping that violates any of the above criteria.

In Step 4 (Chapter 3 Section 3.3.3.4), the participants are required to prepare the strategy and context. The participants are given a score for each correct strategy/context. A correct strategy/context must satisfy (1) the right content, and (2) the right syntactic shape (diamonds for strategies, eclipses for contexts), and (3) be placed in an appropriate location within the diagram. Figure 7.4 provides an example answer for the correct strategy and context identified. A score is not given for a strategy/context that violates any of the above criteria.

7.4.3 Results for the creation of the instance

The results show that all of the 38 participants that have taken information security courses can finish Step 1 and Step 2 achieving 100% accuracy using the criteria pro-

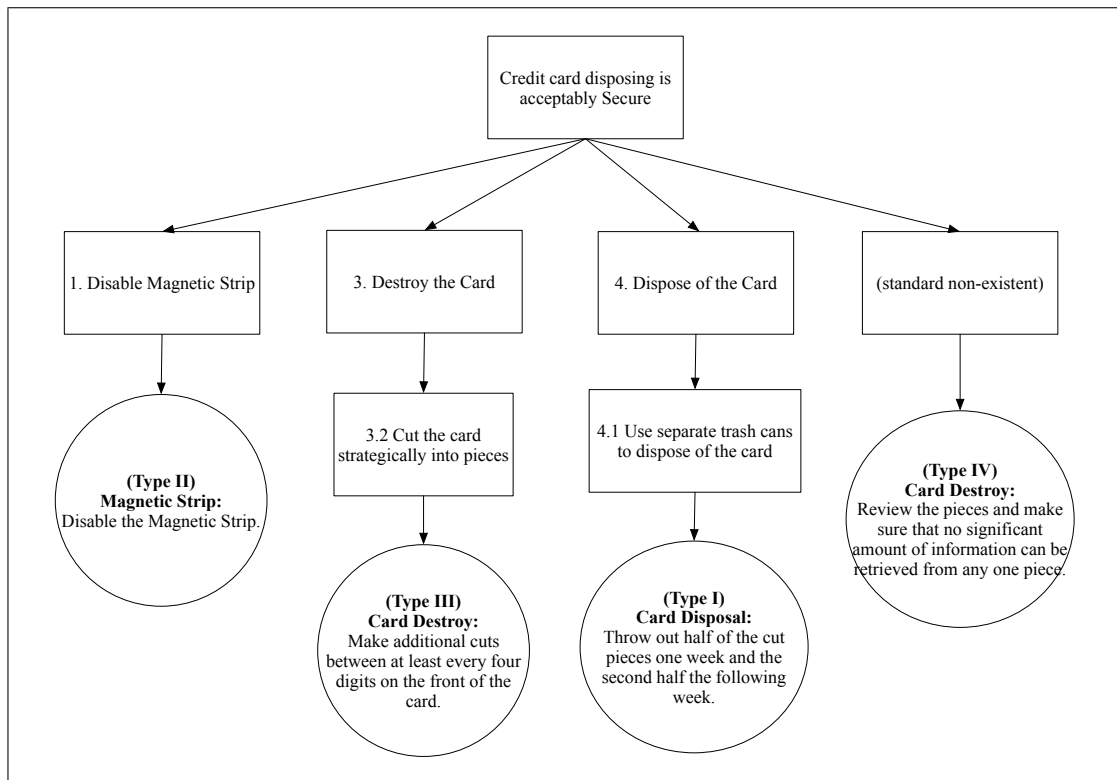


Figure 7.3: Mapping lessons learned to the security requirements of the Credit Card Disposing Case

vided by the security experts in the initial trial. In other words they were able to identify appropriate security goals and lessons learned for the data breach case study. In comparison, 36 out of 37 of participants who have not taken information security related courses could finish Step 1 and Step 2 achieving 100% accuracy. The performance in the third step was more mixed. The average accuracy rate is 2.22 out of 4 for security group, and 1.64 out of 4 for the non-security group. This arguable reveals an underlying problem in making quantitative judgments about the accuracy of arguments in the aftermath of security incidents. Moreover, by using a t-test, we have found statistically significance ($p = 0.007 < 0.05$) in Step 3 between the two groups, which indicates the security group perform better in mapping the lessons learned than the non-security group. In Step 4, the accuracy rate for identifying the strategies is much higher, only one participant failed to identify the correct strategies. For the context, four participants in the security group failed the identification, and one participant in the non-security group failed. There is no statistical significance between the two groups in this step.

Based on the analysis above, we have defined a measurement criteria for the over results. The participants are considered to be successful in creating an instance of the

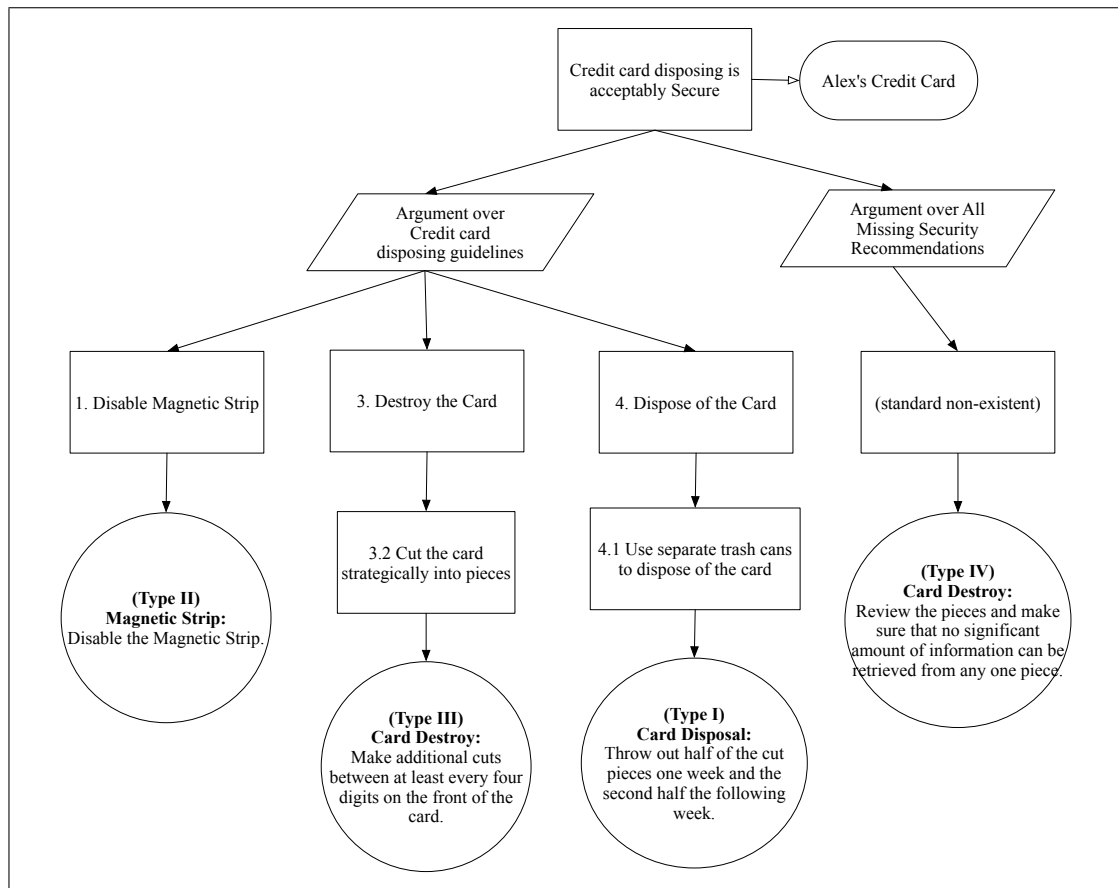


Figure 7.4: Final Credit Card Disposing Instance

GST is he/she satisfies the following criteria.

- The participants can complete step 1 achieving a 100% accuracy rate.
- The participants can complete step 2 achieving a 100% accuracy rate.
- The participants has attempted step 3 by mapping all the lessons learned to the security requirements.
- The participants can complete step 4 achieving a 100% accuracy rate.

The results show that 69 out of 75 participants (92%) can satisfy the above criteria and are therefore successful in creating an instance of the GST.

7.4.4 Results for the post-task questionnaires

The post-task questionnaires were divided into four parts. The first part was intended to collect background information. The second part collected participants' subjective

feedback on the creation of security arguments, structured using the Generic Security Template. We have asked how easy it was for them to complete each step. We have asked for their opinions by using the Five Likert Scales, 1-strongly disagree, 2-disagree, 3-moderate, 4-agree, 5-strongly agree. Table 7.1 lists the average value for each step for different groups. In general the participants complained about the difficulties in Step 3 determining types of lessons learned. For example, one participant in the security group stated, “Sometimes I cannot define what is exclusively related (to a bottom level goal)”, another participant stated, “I don’t know how to determine the types of the Lessons learned”. And they suggested, “Learning from more examples would be helpful”.

	Groups	
	<i>Security</i>	<i>Non-Security</i>
Step 1	4.2895	3.9459
Step 2	4.2895	3.9730
Step 3	3.7895	3.1892
Step 4	3.7838	3.7297

Table 7.1: Average score for different steps of different groups

The third part of the questionnaire provided feedback on workload, using NASA’s Task Load Index (TLX). The model index value ranges from 0 to 20. Table 7.2 has listed the mean value for each dimension for different groups. Statistical significance was found for Task load Index 1 ($p = 0.005 < 0.05$) and Task load Index 2 ($p = 0.043 < 0.05$). This indicates that, the non-security group find it more mentally demanding.

	Groups	
	<i>Security</i>	<i>Non-Security</i>
Taskload Index 1	7.6842	10.4324
Taskload Index 2	7.3947	9.8378
Taskload Index 3	6.1579	7.8919
Taskload Index 4	13.1842	12.8378
Taskload Index 5	8.6842	9.8378

Table 7.2: Average score of different Task Load Index dimentions of different groups

The fourth part of the questionnaire collected more general feedback in terms of ease of use, confidence, satisfaction. We asked questions such as “I am satisfied with the overall experience of the tool”. Again, we have used the Five Likert Scales, to ask for their opinions. Table 7.3 has listed the average value for each aspect for different

groups. There was statistical significance for Ease of Use ($p = 0.037 < 0.05$). The result is interesting that the non-security group find it easier to use than the security group.

	Groups	
	<i>Security</i>	<i>Non-Security</i>
Ease of Use	3.8421	3.4054
Confidence to Use	3.5789	3.3784
Satisfaction	3.7895	3.8108

Table 7.3: Average score for different evaluation aspects for different groups

In this part, we have also let the participants document the estimated time needed to complete the whole tasks, for the security group, the time ranges from 30 minutes to 240 minutes with a mean time of 103 minutes, in comparison, for the non-security group, the time ranges from 30 minutes to 900 minutes with a mean time of 157 minutes however, there is no statistically difference found between the two groups.

7.5 External and internal threats

7.5.1 Internal validity

Internal validity is concerned about the cause-effect relationships induced from the study. *Maturity effects*, the participants took away the task and performed at their own pace. We do not think there is a threat that the participants would tend to be bored and performed worse towards the end of this task. *Learning effect*, there was not a learning effect in this experiment as there was only one treatment. *Testing effects*, all participants have studied the same training material and all of them have attended the same GSN training courses. There might be cheating because the students took away the task. However, this task was not assessed and the participants were asked to work independently. *Instrument effects*, the participants were given the same type of task and the answers were evaluated by the same evaluator using the same marking scheme.

7.5.2 External validity

External validity is the possibility to generalise the results beyond the current experiment. We addressed these concerns by selecting a good number (81) of students with a computing science background. However, the security incident used in this study is

much simpler than the real world security incidents [14–16, 44] in healthcare organisations. More efforts will be needed to structure lessons learned from complex security incidents in real practice.

7.6 Discussion

We can conclude from this study that the participants with computer science background can achieve a high accuracy rate in preparing the goal structure, lessons learned and strategies and context of the Generic Security Template in a customised evaluation. Although they have demonstrated varied mapping of the lessons learned to the goals in Step 3, the subjective feedback shows that the guidance on the mapping does help them decide different types of the lessons learned. However, it is still difficult for them to generate the same graphical overview even following the same rules. This is due to the subjective nature of the GSN, that allows the template to be further reviewed and discussed by others. Moreover, the subjective feedback from the participants shows that they are generally satisfied with the experience of the creation process, although they found some difficulties in completing Step 3 on mapping the lessons learned to the goal structure.

7.7 Summary

This chapter evaluated the improved Generic Security Template and investigated whether the use of this approach can be generalised to a large number of users with a computer science background. The results of an empirical study with 81 university students show that the students with a computer science background can create a Generic Security Template and they are generally satisfied with the experience of this approach. However, the study with university students to structure simple security incident can hardly reflect the use of the GST in real industry practice. Future work should focus on the application of the GST in healthcare.

Chapter 8

Investigation on the Transferability of Lessons using the Generic Security Template in Healthcare Systems - An Industrial Evaluation

The Generic Security Template provides a way to feed back lessons identified from security incidents to the ISMS. Chapter 6 presented a preliminary industrial evaluation of the Generic Security Template to identify its strengths and weakness through interviews with Chinese healthcare professionals. Chapter 7 evaluated the improved Generic Security Template with university students. This chapter expands the work and investigate how lessons presented by the Generic Security Template can inform the implementation of security standard. In particular, we investigate how lessons identified from security incidents in different countries can be transferred to the redacted central hospital to inform their implementation of security standards.

This chapter is divided into the following sections. Section 8.1 outlines the evaluation plan, including the objectives of the study and the target group. Section 8.2 introduces the study process which includes two main steps, transfer lessons from one strategy (e.g. FISCAM) to another (e.g. GB/T22239) and determines acceptance of lessons transferred from healthcare organisations in different countries. Section 8.3 analyses the results from the first step on the transferability of lessons learned. Section 8.4 analyses the results from the second step on the acceptance of the lessons learned. Section 8.5 reports on further customisation requirements. Section 8.6 presented the revised Generic Security Template Pattern. Section 8.7 discusses the implications for

healthcare. Section 8.8 summarises this chapter.

8.1 Study design

8.1.1 Study objectives

The interviews with healthcare professionals in China (Chapter 6) provided initial insights into the application of our approach. However, we were also anxious to look beyond subjective impressions to provide more direct evidence about whether or not security lessons can be transferred between healthcare organisations in different countries. In particular, we have used three instances of the Generic Security Template, which are the VA 2006, VA 2007 and Shenzhen data leakage incident. The aim here was to investigate whether Chinese healthcare professionals could transfer security lessons learned from these incidents into their own working context. We, therefore, conducted an in-depth study with Chinese participants to gather a range of views about the utility of our approach. The objectives of this study are outlined below,

8.1.2 Target organisation

The redacted central hospital was used for a preliminary study in applying the Generic Security Template (Chapter 6). They expressed their interest in the approach. This allows us to continue this study using focus group in the redacted central hospital.

We conducted a group study that involves different stakeholders including healthcare professionals, and IT professionals who can make the final decision within their ISMS. We have chosen focus group because,

(1) Nature of this practical task. The group was asked to identify lessons that might be re-used to increase the protection of patient data. In the redacted central hospital, whenever a decision in information security has to be made, different stakeholders in the organisation are gathered together to discuss the issues. The final decision will be made by the IT manager based on these different views. The relevant IT manager within the hospital agreed to participate in the session.

(2) The difficulty of agreement on the mapping of lessons learned. In the pilot industrial study, users identified many different ways of mapping lessons to policies, standards and guidance. This reflects the subjective processes that affect the construction of our graphical maps. GSN structures can serve as a platform for communication

and facilitate different parties in coming to agreement [7]; group work is suitable to stimulate such activities.

(3) The exploratory nature of this study. Interaction among group participants often reduces the amount of interaction needed between the moderator and the individual members of the group. In this way, the dynamics within the focus group can reduce the researchers' influence on the interview process [224]. Focus groups can stimulate thinking and verbal contributions.

This group consists of six people, three healthcare professionals, two IT experts and one IT manager. They are different stakeholders in protecting patient data and the potential target users of the Generic Security Template. The researcher played the role of moderator. The moderator addresses a number of issues for discussion and assures that the discussion remains on the subject of interest. Interference with the discussion is kept to a minimum, which is motivated by the aim to create a communication situation which bears close resemblance to "naturally occurring interaction" [225].

8.2 The study process

In the study, group participants were asked to identify lessons that they could apply from our graph of those instances of the Generic Security Template. To avoid fatigue the meeting was divided into two sessions. Each one lasted for approximately 1.5 hours. In both sessions, an IT engineer from the IT department accompanied the researcher and together they maintained field notes to document the group discussion.

8.2.1 Demonstration of the Generic Security Template

The participants were required to read the Instruction on the Creation of the Generic Security Template (Appendix D.1) before this study. And then the research conductor presented the three instances of the Generic Security Template to the participants. They had the opportunities to ask questions before the group discussion.

8.2.2 Execution of the group study - first session

As the security management of the redacted central hospital has followed the Chinese standard, GB/T22239. They decided to replace the goal structure of the VA 2006 and VA 2007 data leakage incident, which was FISCAM, with GB/T22239. In the study, group participants discussed how to map lessons learned in the instances of the Generic

Security Templates for the VA 2006 and VA 2007 data leakage incident to different levels of security requirements in GB/T 22239. This study lasted for 1.5 hour.

8.2.3 Execution of the group study - second session

In the second session, the study was conducted by traversing each of the lessons learned in the instances of the Generic Security Templates produced in the first session. Participants were asked to discuss and decide on the acceptance of lessons in the revised Generic Security Template. The discussion lasted for 1.5 hour.

A set of group study guidelines (open-ended questions) was developed for the moderator including probes designed to re-focus the discussion if necessary.

- Does your organisation have the (e.g. “Sensitive Information”) issue?
- Do you think this recommendation is helpful for your organisation?
- Would you be able to apply this recommendation?
- What are the barriers for you to apply this recommendation?

In both of the above two sessions, a security engineer was invited to accompany the researcher in recording field notes of the group discussion. This is to ensure the completeness of the information documented, as the research conductor has to play the role of moderator and may miss some information during this process.

8.3 Execution of the group study - first session

8.3.1 Transferring the lessons learned

As mentioned, the Chinese group, chose to focus on the provisions within GB/T22239 that might help to avoid any similar incidents in their hospital. This process lasted over an hour and included a detailed analysis of the clauses in GB/T22239 as well as the VA incident.

During this process, they followed the steps to apply the Generic Security Template (Chapter 3 Section 3.3.3) to structure the lessons learned. They have skipped “Step 1: Prepare the goal structure of the Generic Security Template” and “Step 2: Identify the lessons learned from the security incident”, because the goal structure and lessons learned are readily available. By following “Step 3: Map the lessons learned to the

goals (security requirements) in the goal structure (security standard)”, they decided the mapping of lessons to different levels of the goals (security requirements) in the goal structure (security standard). By following “Step 4: Elaborate the Context and Strategies”, they have set the strategy as “Argument over GB/T22239” and context as “the redacted central hospital”. Previous empirical studies with students (Chapter 7) have identified the difficulties in Step 3 about mapping the lessons to different levels of the goals. Section 8.3.2 highlights this step and reports the findings.

8.3.2 Types of lessons learned and rules of mapping

Depending on their relation with the goals, the lessons learned have been divided into different types. Recall the definition of four different types of the lessons learned and the rules to decide the mapping that we have developed in Chapter 6,

Types of lessons learned and rules of mapping

Starting from the bottom-level goals in the goal structure, (Type I) if a lesson learned is related exclusively to a bottom-level goal, it is defined as Type I. Then this lesson learned should be mapped to this bottom-level goal. (Type II) If a lesson learned is related to more than one bottom-level goals in the goal structure, it is defined as Type II. Then this lesson learned should be mapped to the nearest parent goal where those bottom-level goals share the same parent goal. (Type III) If a lesson learned is related to none of the bottom-level goal, go up to check other goals, check and decide whether it is related to a higher level goal in the structure. If yes, it is defined as Type III, this lesson learned should be mapped to this related goal. This indicates a probably missing aspect of a higher level goal. (Type IV) If a lesson learned is related to none of the goals in the goal structure, it is defined as Type IV, then a new goal named “(Standard non-existent)” should be created to link this lessons learned to the top goal. This indicates a missing aspect of the whole security management guidelines or standards.

Below are the examples of lessons learned Type I, II, III and IV that are cited from the real world security incidents used in our industrial evaluation. In particular, examples of Type I, III and IV are cited from Figure 8.1; example of Type II is cited from Figure 8.3. The goals (security requirements) for those cases are from the GB/T22239. In the following examples, different types of lessons learned have been mapped to different levels of security requirements of GB/T22239.

Type I

Lesson learned (Figure 8.1)

Sensitive Information: Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage.

Security Requirement bottom level(From GB/T22239)

.....

8.1.5.2.a Use encryption or other protective measures for system data management, information identification, and the transmit of critical business data.

8.1.5.2.b Use encryption or other protective measures for system data management, information identification, and the storage of critical business data.

8.1.5.2.c Provide dedicated communication protocol or secure communications protocol services for important communications channels. Avoid destruction of data confidentiality from the general protocol-based attacks.

.....

Decision on Mapping

The lesson learned is found to be exclusively related to bottom level security goal 8.1.5.2.b, therefore, it should map to 8.1.5.2.b. It indicates if this lesson learned is ignored, the goal 8.1.5.2.b. would be affected.

Type II

Lesson learned (Figure 8.3)

Security Training: Establish and execute security training programs by following the security standard.

Security Requirement bottom level - 1

8.2.3.4 Security awareness education and training.

Security Requirement bottom level

8.2.3.4.a Security awareness training, position related technical and security skills needs to be educated to all staff.

8.2.3.4.b Security responsibility and punitive measures need to be documented and informed to the responsible staff. Disciplinary actions need to be taken to people violating security policies.

8.2.3.4.c Security education and training needs to be documented regularly. Training including basic security knowledge, position operational procedure needs to be designed for different positions.

8.2.3.4.d Security education and training needs to be examined, and the results are placed on file.

.....

Decision on Mapping

The lesson learned is found to be related to all of the listed bottom-level goals, therefore, it should map to their parent goal 8.2.3.4. It indicates if this lesson learned is ignored, the goal 8.2.3.4 or its sub-goals would be affected.

Type III

Lesson learned (Figure 8.1)

Position Description: Re-evaluate and correct position sensitivity levels.

Security Requirement bottom level - 1

8.2.2.1 Position description (G4)

Security Requirement bottom level

8.2.2.1.a Establish functions management structure for information security management. Establish the job role for security officer, security management in charge of all aspects of security management and define the responsibility of each position.

8.2.2.1.b Establish the job role for system administrators, network administrators, security administrators and define the responsibility of each position.

8.2.2.1.c Established information security management committee or leadership team, led by the highest leadership of the unit in charge of the appointment or grant.

8.2.2.1.d Develop clear institutional responsibilities of various departments and positions, division of labor and skill requirements.

Decision on Mapping

The lesson is found to be related to none of the bottom-level goals, e.g. 8.2.2.1.a....., however it is related to a higher level goal 8.2.2.1. This lesson should be mapped to 8.2.2.1. It indicates this lesson is probably missing from the goal 8.2.2.1.

Type IV***Lesson learned*** (Figure 8.1)

Risk Analysis: Develop and issue Government-wide risk analysis criteria.

New Security Requirement

(Standard non-existent): Government-wide risk analysis criteria is addressed.

Decision on Mapping

The lesson learned is found to be related to none of the security requirements of GB/T22239, a new goal, Standard non-existent, should be created addressing this recommendation. It indicates this lesson learned is probably missing from GB/T22239.

8.3.3 The customised GST instances

Figure 8.1, 8.2 and 8.3 show the resulting instances of the Generic Security Template for the incidents by following the rules in section 8.3.2.

The process of mapping between the US case study and the context in Chinese healthcare yielded some significant insights. For instance, in the VA 2007 data leakage incident, one of them which is “Risk Analysis”, has changed to be under the strategy “Argument over All missing Recommendations”. It identifies a new security requirement that is probably missed by GB/T22239. Some of the lessons learned identified from VA 2006/2007 data leakage incident can be mapped to a deeper level, which is the bottom level of the GB/T22239. For example, the lessons learned “Sensitive Information” from the VA 2006 data leakage incident is mapped to the goal (security requirement) 8.1.5.2.b as is shown in Figure 8.2, however, a similar lessons learned in the Shenzhen data leakage incident “Sensitive Data” is mapped to a higher level goal (security requirement) 8.1.5.2. This to some extent indicates the different maturity level of the healthcare system security management in the VA and in China.

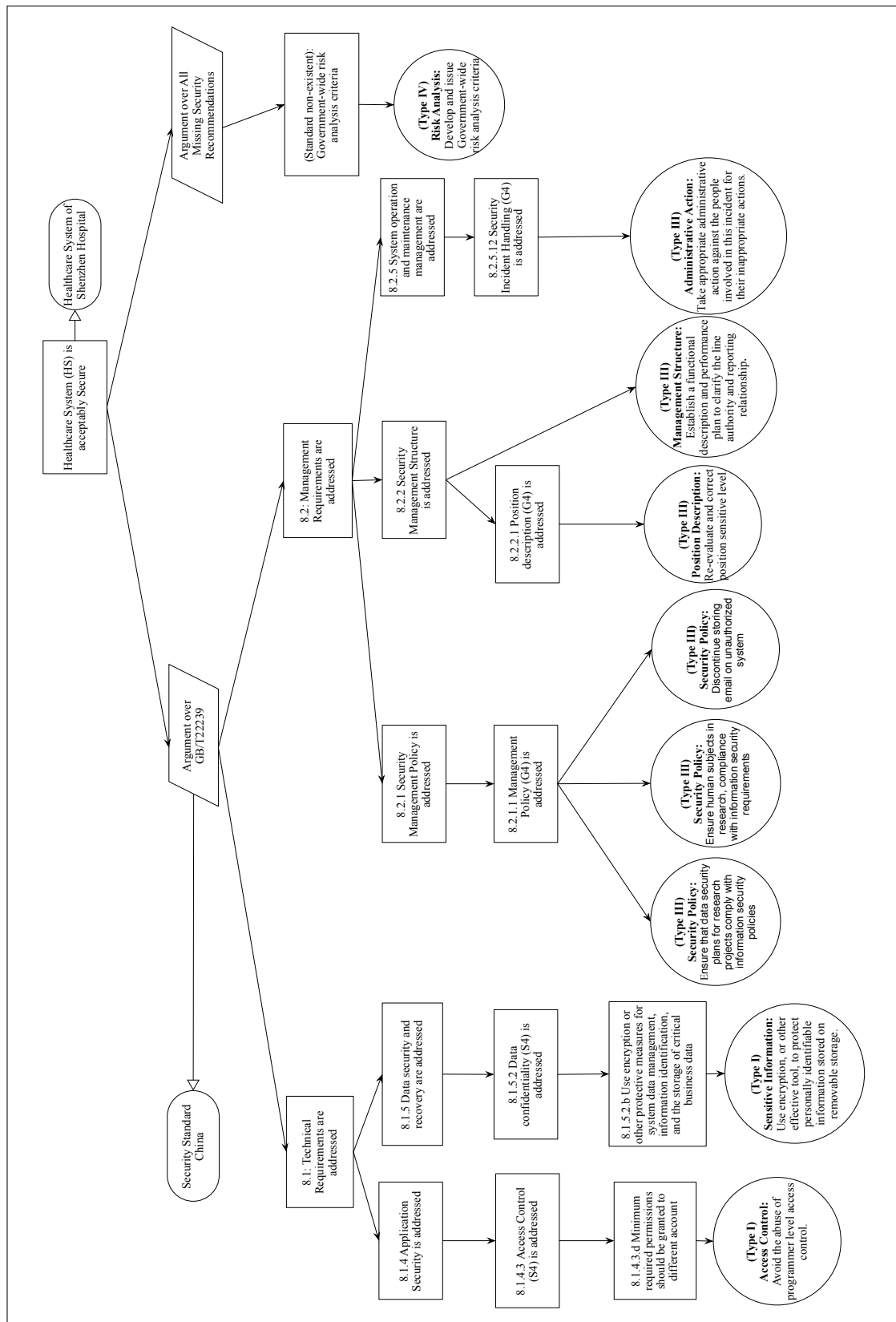


Figure 8.1: Instance of the Generic Security Template VA 2007 - customised by replacing the security standard

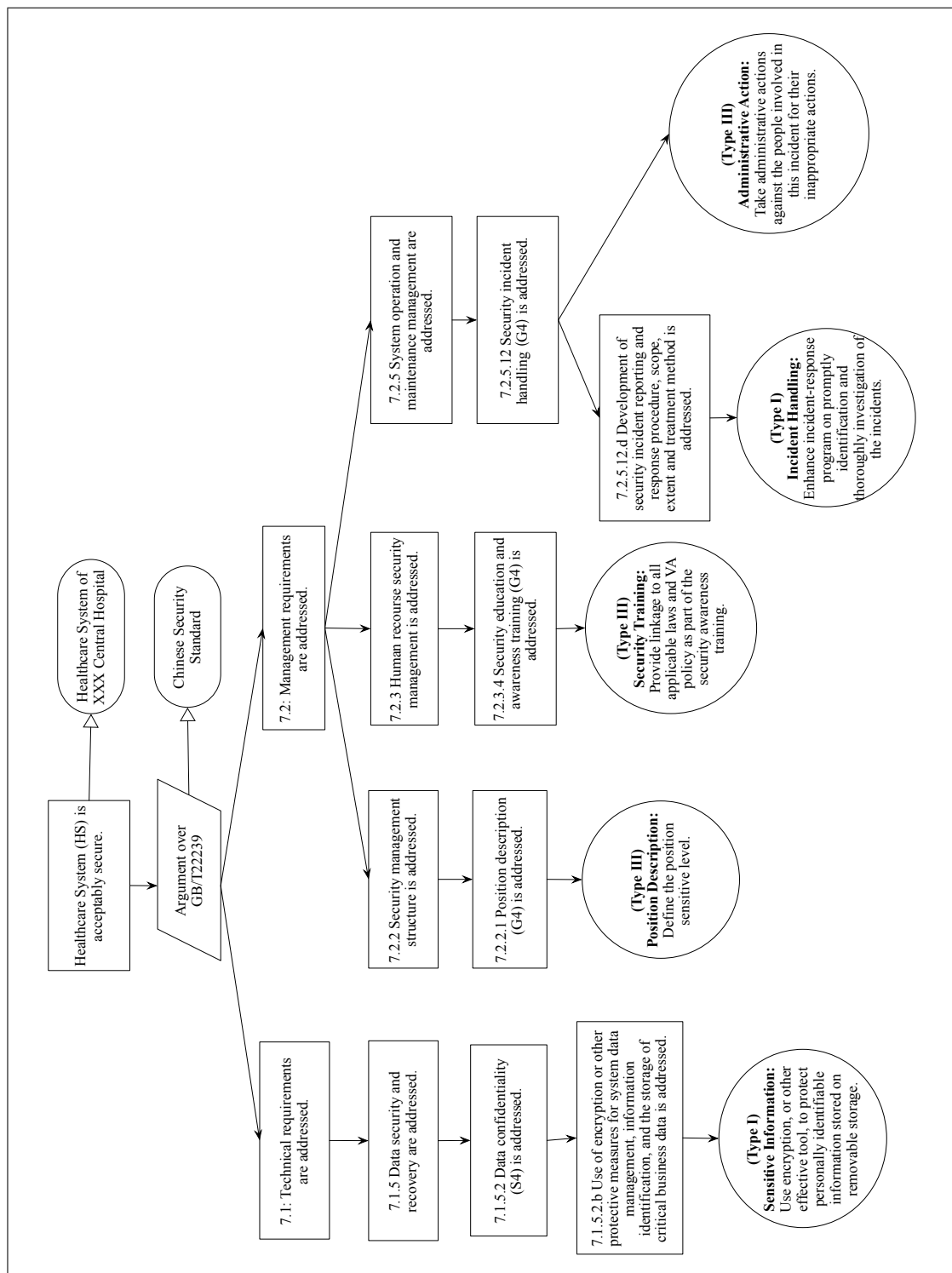


Figure 8.2: Instance of the Generic Security Template VA 2006 - customised by replacing the security standard

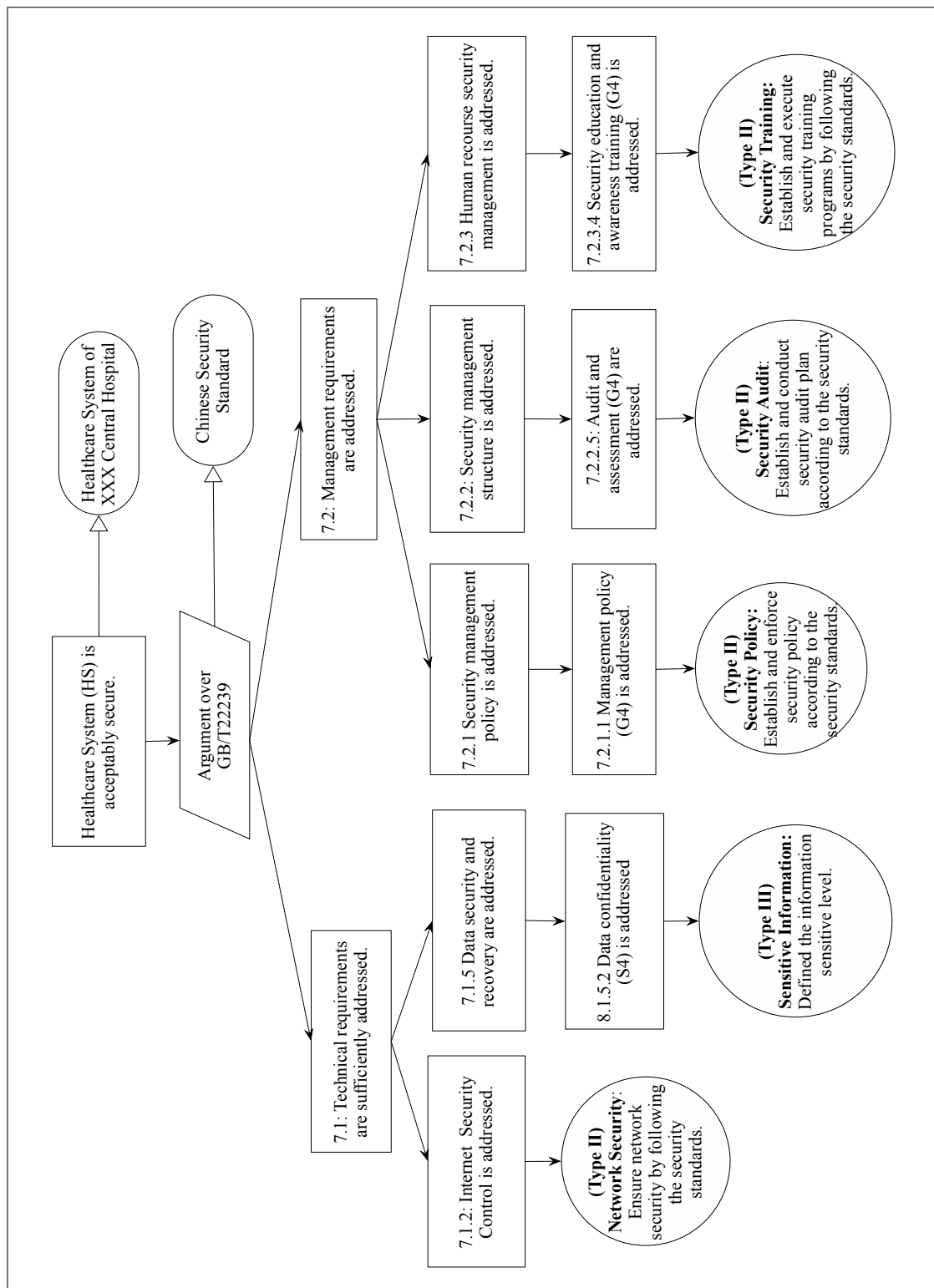


Figure 8.3: Instance of the Generic Security Template Shenzhen

The participants expressed that they have experienced disagreements between different stakeholders while deciding the mapping of lessons learned to the goals, typically on deciding the level of the goals (security requirements) that the lessons should map to. The use of the GSN has been proved to be successful in enabling debate and agreement on the safety argument [7]. The group stated that this group work helped them come to an agreement and better understand the reasoning between the lessons learned and the goals.

8.4 Execution of the group study - second session

In the first session, the focus group related the findings from the VA case study to the provisions in the Chinese standard GB/T22239. They were not asked to consider whether they could be implemented within their own healthcare organisation. In contrast, the second session traversed the new diagram to identify any barriers to the application of the lessons derived from the VA case study. These discussions lasted for a further hour.

8.4.1 Acceptance of the lessons learned

The group followed an identifiable process in assessing the acceptability of lessons within their own organisation. They began by assessing whether each issue that arose for the VA was also a significant concern in their hospital. They would then decide whether to accept the recommendation, or customise lessons learned to suit their own context. The acceptance of the lessons are categorized into the following six types reflected in Figure 8.4, 8.5, 8.6. We take the VA 2007 data leakage incident, shown in 8.5 as an example to explain the organisation's decision on the acceptance of the lessons learned. More details on the acceptance of the lessons learned for the VA 2006 data leakage incident and Shenzhen data leakage incident are provided in Appendix E,

Implemented. Some of the lessons identified from the VA 2007 case study had already been implemented within the host organisation. For example, the “Security Policy” recommendation to “Ensure that data security plans for research projects comply with information security policies”. In particular, an audit might be conducted to confirm this finding.

Implemented with customisation. Some of the lessons identified within the VA 2007 case study had already been addressed by the organisation but with a slightly

different emphasis or approach. For example, for the “Security Policy” recommendation to “Ensure the handling of human subjects in research, complies with HIPAA rules;” In the Chinese context, the hospital required that electronic records relating to human subjects were held in compliance with the relevant national data protection act “China Personal Information Protection Act” [226].

Implementable. Some of the issues identified in the VA 2007 incident had not yet been addressed by the Chinese hospital, however, they accepted the need to consider this finding. For example, the VA report recommended changes in the “Management Structure” to “Establish an accurate functional description and performance plan to clarify the line authority and reporting relationship”. The Chinese focus group felt that it would be useful to review their existing practices using the insights derived from the US case study data breach.

Implementable with customisation. Some of the security issues identified in the VA case study had not been addressed by the organisation, however, the focus group felt that they could not be implemented without considerable changes within their own organisation. For example, the VA report identified the need to “Re-evaluate and correct position sensitivity levels”. This process had not been formalized with the Chinese hospital, hence the focus group rephrased it as “Define position sensitive levels”.

Reserved for future use. The penultimate category describes findings that could be re-applied in China but their implementation would take a considerable period of time, for instance where the security management system was not sufficiently mature. For example, the VA recommended that staff “Use encryption, or other effective tools, to protect personally identifiable information stored on removable storage”. The Chinese hospital forbids the use of removable media hence this recommendation is not immediately applicable. However, the group could envisage a time when this requirement might be relaxed. If removable media were to be permitted then the VA recommendation would be an essential requirement for future security.

Implementation unnecessary. Some of the US VA recommendations could not be applied in the Chinese healthcare organisation. For example, the previous incident report recommended action to “Develop and issue Government-wide risk analysis criteria”. Currently, the redacted central hospital interacts with government wide systems, including the Chinese national insurance system. However, they felt that this recommendation could only be implemented at government level, hence it was not a subject they felt was in their area of responsibility.

8.4.2 The customised GST instances

The above acceptance types have been reflected in the revised Generic Security Template as is shown in Figure 8.4, 8.5 and 8.6.

A comparison of the Generic Security Template of the VA 2006, VA 2007 and Shenzhen security incident reveals that, the redacted central hospital is more likely to accept recommendations from the Shenzhen security incident. The acceptance types are implemented, implemented with customisation, and implementable. This might be due to the similarity of the healthcare system settings within the same country. On the other hand, the VA security incidents have some additional acceptance types, which are reserved for future use and implementation unnecessary. For example, the lessons learned “Sensitive Information: Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage” is reserved for future use because the organisation currently does not allow any kind of patient data to be stored in removable storage. The lessons learned “Security Policy: Discontinue storing email on unauthorized system” is reserved for future use because the organisation currently does not use internal email systems, which indicates different system settings between different countries. The lessons learned “Risk Analysis: Develop and issue Government-wide risk analysis criteria” are implementation unnecessary because the organisation believes it is the governments’ responsibility to develop and issue government-wide risk analysis criteria.

As we have seen, the development of a specific security incident map from the Generic Security Template helps organisations consider their own practices and to assess whether applicable security standards address the concerns raised in previous breaches. Again, in this process, participants stated the GST provides a platform for discussion and helped them come to the final decision on acceptance of lessons learned.

8.5 Other customisation requirements - multi-view

The organisation identified some other customisation requirements of the Generic Security Template, such as multi-view approach, a requirement raised in Chapter 6. The Generic Security Template is then further customised and those new features will be considered in the future design of the Generic Security Template. Identifiers that document the target groups are added to the Generic Security Template and the adjusted Generic Security Templates are produced. The target groups were classified into three,

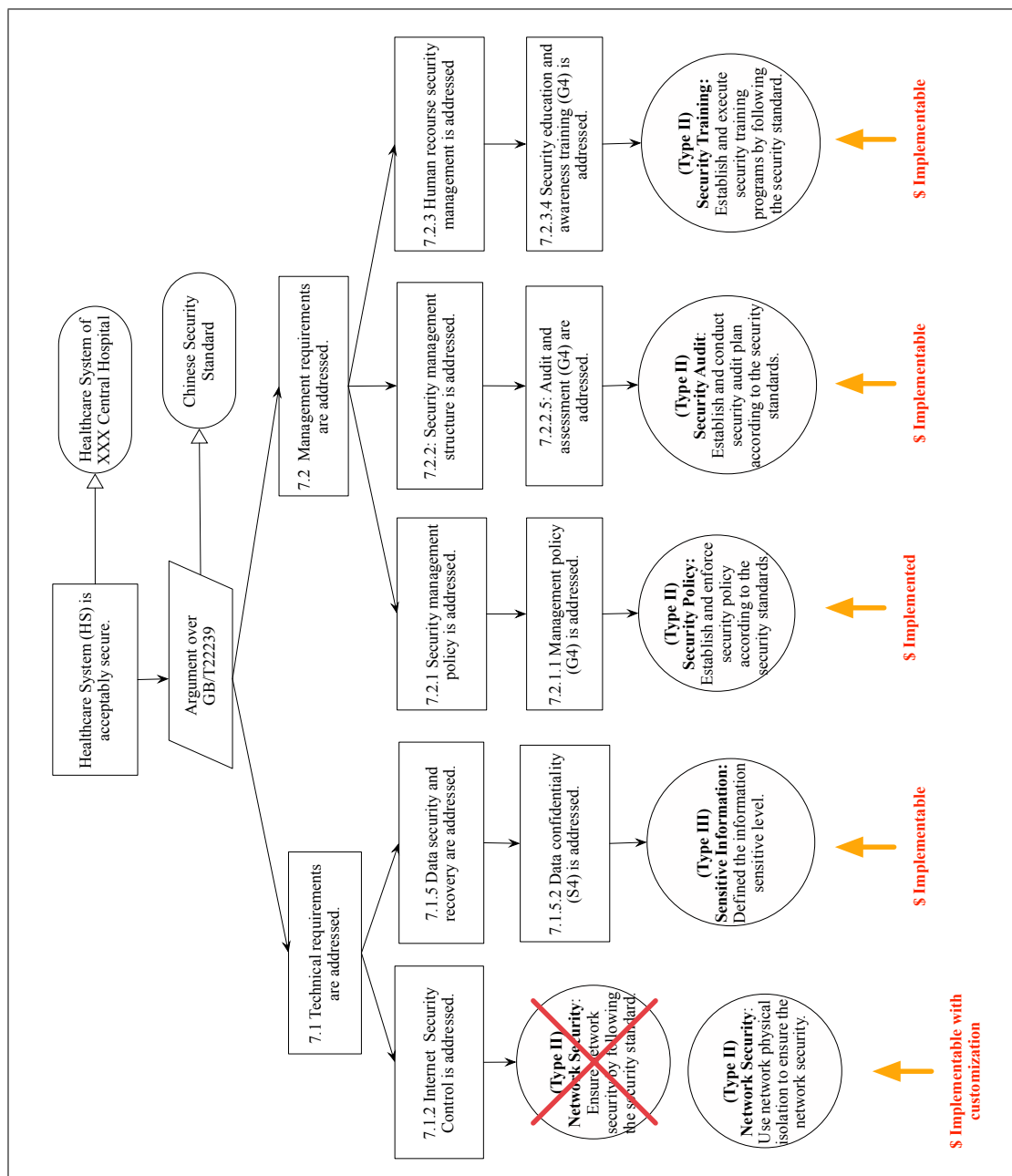


Figure 8.4: Instance of the Generic Security Template Shenzhen 2008 - customised by implementation types

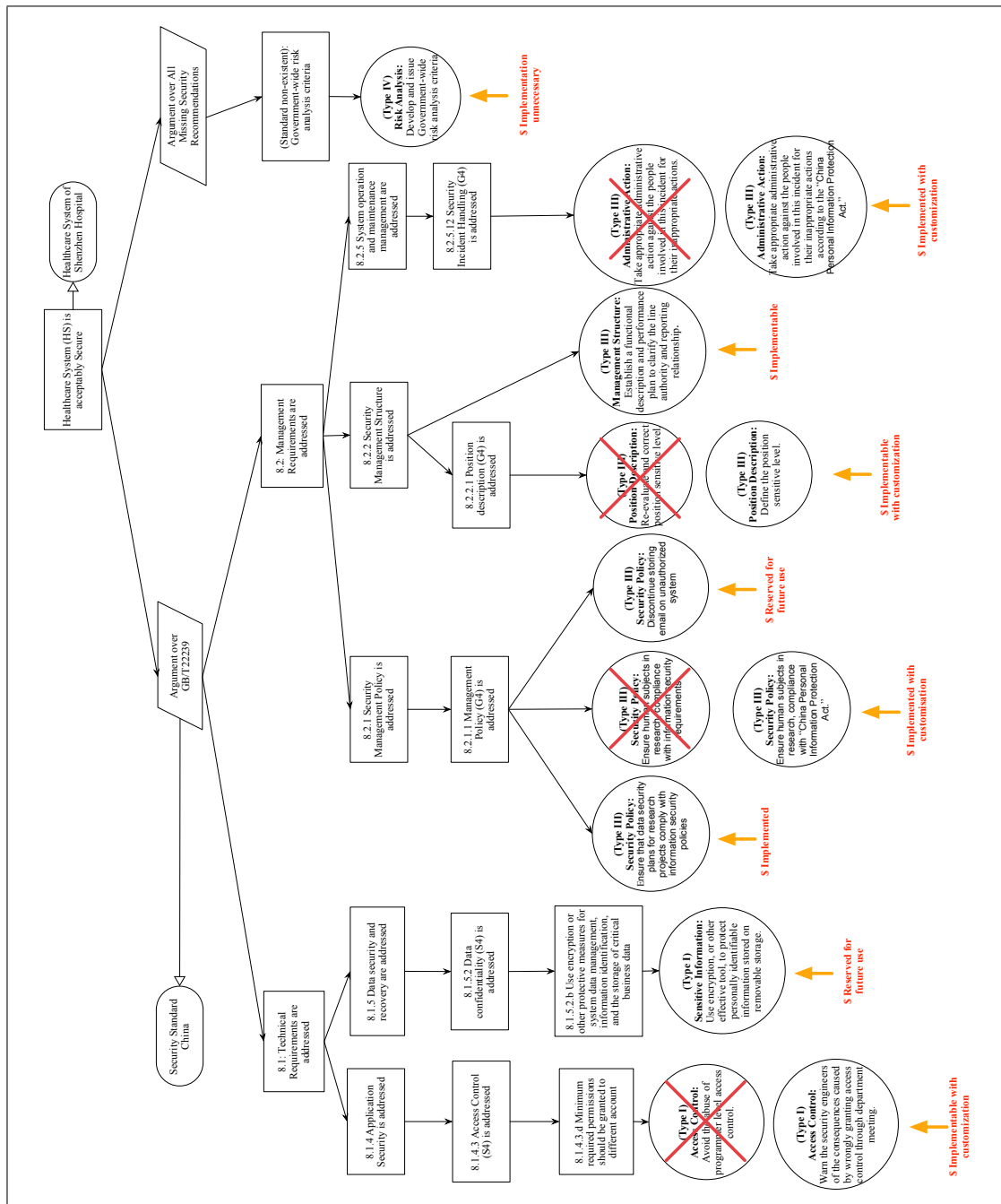


Figure 8.5: Instance of the Generic Security Template VA 2007 - customised by implementation types

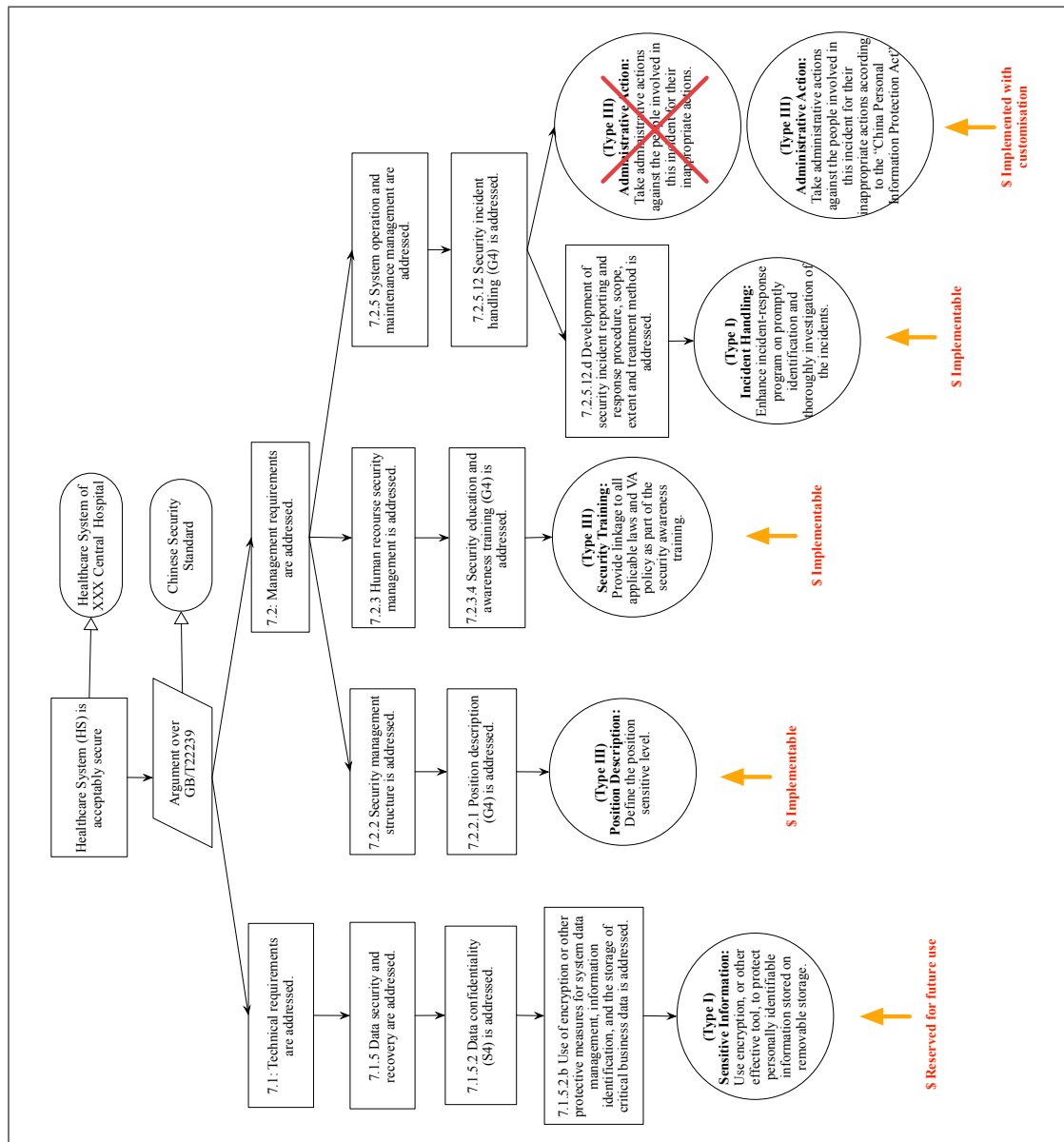


Figure 8.6: Instance of the Generic Security Template VA 2006 - customised by implementation types

IT security management, IT security engineer and healthcare professionals. Those changes are reflected in Figure 8.7. Similar requirement has been identified in safety area and multi-view safety cases have been proposed to address it [227]. The objective is to filter information of different stakeholders' interest and reduce complexity of the safety argument. However, future work needs to evaluating the concept of multi-view using real world case studies and peers review [227].

8.6 The revised Generic Security Template Pattern

The Generic Security Template Pattern was revised to reflect the improvements of the GST throughout the previous evaluations and the customisation requirements. The adjusted Generic Security Template Pattern is shown in Figure 8.8. There are also some identifiers attached to the lessons learned notation, including the *Recommendation Acceptance Identifiers*, shown in Figure 8.4, 8.5, 8.6 and the *Multi-view Identifiers*, shown in Figure 8.7. However, they are not reflected in the revised Generic Security Template Pattern. We suggest that future software support can simplify the display of the Generic Security Template by making those identifiers properties of lessons learned. Users can set those properties during customisation and use them as filters to display the desired lessons.

There are usually more than one security standards/policies/guidelines within one organisation. The organisational information security management were achieved through a combined efforts of the enforcement of different management standards/policies/guidelines [107, 228, 229]. The Generic Security Template Pattern can be applied to map security lessons to individual standard/policie/guideline, producing different instances of the Generic Security Template. An integration of those instances together contributes to the information security management of the organisation.

8.7 Discussion

The evaluation can be considered on several different levels, (1) demonstrating the acceptability of this approach in feeding back the lessons learned to the ISMS; (2) demonstrating the benefits of this approach over others in feeding back the lessons learned to the ISMS. Since success in (1) can provide the basis for future evaluation, which is a precursor to success at (2), therefore the evaluation in this chapter is focused on (1). This is identical to Kelly's choices in evaluating the GSN (T. P. Kelly, 1999).

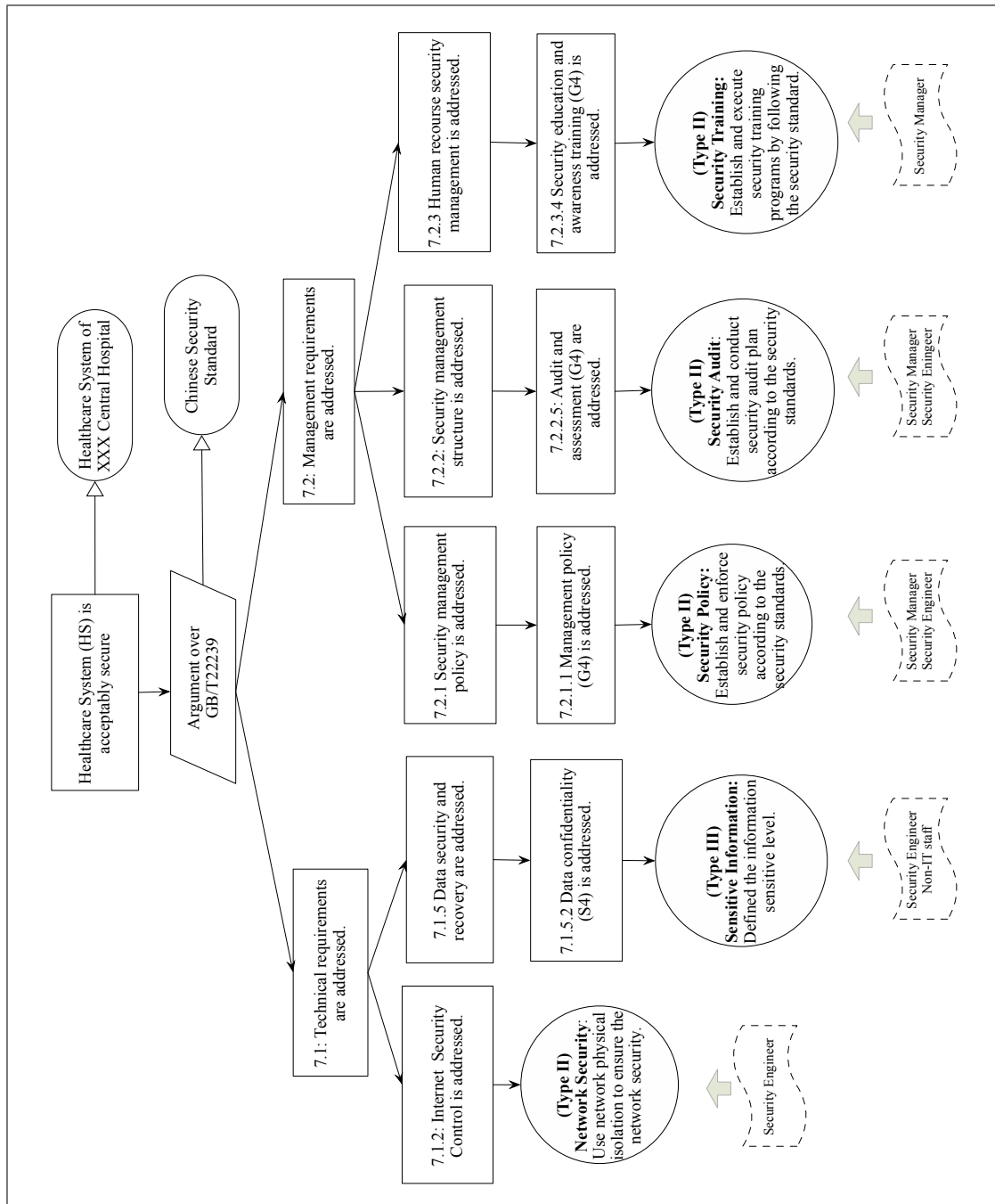


Figure 8.7: Instance of the Generic Security Template Shenzhen - customised after adding the multi-view identifiers

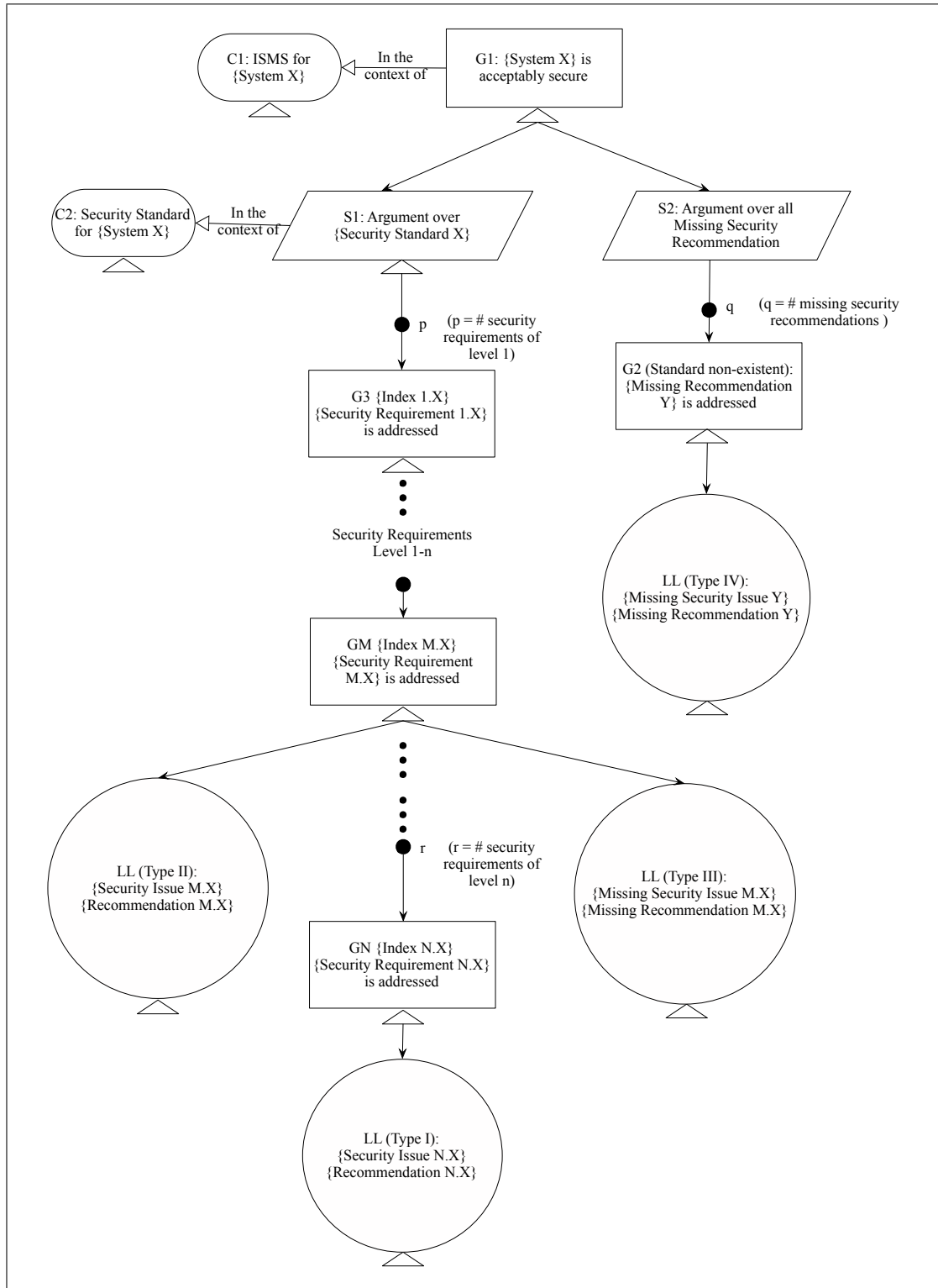


Figure 8.8: The adjusted Generic Security Template Pattern after a series of customization

Chapter 6 has identified the potential benefits for the healthcare organisation to apply this approach over their existing mechanisms. This chapter extends the work and gets more direct evidence about the application of the GST.

By using three instances of the Generic Security Template, we have found that the lessons learned from incidents in other healthcare organisations both at home and abroad can be transferred into the redacted central hospital. This study provides a successful example of a practical case, that forms the foundational work to generalise the use of this approach to other healthcare organisations. It has implications and contributes to the sharing of the lessons learned from security incidents globally in feeding back information to ISMS.

The transferability of the lessons learned from the Generic Security Template of these cases demonstrates a number of key issues. For example, the VA 2006 included lessons that could not be mapped to the co-responding security requirements in the Chinese security standards. This has potential implications for enriching security standards in China. Moreover, we have noticed the differences in the acceptance of lessons learned from security incidents at home and abroad. The redacted central hospital is more likely to accept lessons from the Shenzhen data leakage incident. This might be due to the similarity of the healthcare system settings. This finding has implications for future research on the transferability of lessons learned from cross-country security incidents.

Since we have performed the study within one healthcare organisation, the findings may not reflect the results in other healthcare organisations around the globe. However, the experience gained from this study provides the basis for future work in conducting the same study in other healthcare organisations.

8.8 Summary

This chapter conducted an in-depth study to find out how lessons learned can be fed back into improvements of security standards using the Generic Security Template. In particular, we use security incidents from different countries to find out how lessons learned can be transferred to the redacted central hospital to inform the implementation of security standards. The findings show that learning in other healthcare organisation both at home and abroad can be transferred. We also identified the process of transferability using the Generic Security Template. This has implication for the exchange of security lessons globally. Moreover, other customisation requirements were raised

and collected in this chapter such as the recommendation acceptance identifiers and the multi-view identifiers. Those will be considered in the design of the Generic Security Template in future.

Chapter 9

Conclusion

This dissertation proposes an approach, the Generic Security Template, to structure the insights derived from security incidents in healthcare organisations. We have drawn insights from empirical studies examining the usability of the Generic Security Template and industrial case studies. The remainder of this section discusses the contributions and conclusions of the dissertation.

9.1 Conclusions

The dissertation hypothesis is “The Goal Structuring Notations (GSN) can be used to depict the lessons learned from security incidents and map them to the security requirements for an Information Security Management System. We define the resulting graphical overview as the Generic Security Template (GST). We argue that the GST can assist users to identify the lessons learned from security incidents and can be applied to structure the insights derived from specific security incident. The GST is acceptable in a healthcare organisation and can be used to feed back the lessons learned to Information Security Management Systems in healthcare.”

Based on industrial and academic motivations (Chapter 1, 2), the Generic Security Template (Chapter 3) was proposed, aiming to feed back lessons identified from security incidents to Information Security Management Systems (ISMS). In particular, it adapted the Goal Structuring Notations (GSN) to depict the lessons learned from security incidents and map them to the security requirements for an Information Security Management System. The suitability has been tested and instances of the GST (Chapter 4) have been produced based on the analysis of four security incidents in the US, UK and China. This approach has been evaluated through empirical study (Chapter 5)

by assessing its usability in assisting users to identify the lessons learned from security incidents in terms of accuracy, efficiency and ease of use. An empirical study with a group of 24 university students with diversified backgrounds found that the Generic Security Template can help improve the accuracy in identifying the lessons learned from the security incident reports and reduce the mental effort in this process. Although this study yields insights into difficulties that the stakeholders face when trying to understand security incident reports, this evaluation does not reflect real practice. Therefore, industrial evaluations (Chapter 6) of the Generic Security Template have been conducted to test the acceptability with people experienced in dealing with patient data in healthcare organisations. Strengths and weaknesses of the Generic Security Template were discussed, and application scenarios were identified based on the requirements of different stakeholders. The Generic Security Template has been improved after a series of evaluations and the improved Generic Security Template has been evaluated with a larger user group (81 students) (Chapter 7) to show that users with a computer science background can apply the Generic Security Template to structure the insights from the security incidents. The Generic Security Template was finally applied in a healthcare organisation (Chapter 8) in China and the results show that lessons from security incidents in the US and China can be transferred to a healthcare organisation in China using the Generic Security Template. The Generic Security Template has been evaluated and improved throughout the above-mentioned empirical and industrial evaluations. A detailed instruction on the finalised Generic Security Template can be found in Appendix D.

9.1.1 Dissertation research question 1

The answer to research question 1 “Can the Generic Security Templates be created for structuring the lessons learned from security incidents?” is yes. In Chapter 4, we have studied four security incidents from around the global, including the VA data leakage 2006, 2007, Shenzhen data leakage incident, and NHS Surrey IT asset disposal incident. The instances of the Generic Security Template have been created for each security incident. After a series of healthcare (Chapter 6) and practical (Chapter 5) evaluations and improvements, Chapter 7 had evaluated the improved Generic Security Template with a larger user group that has 81 university students with a computer science background, to find out whether university students with a computer science background can use this approach to create a GST in a continued study. The results

show that almost all of them can create a generic security template, although they have difficulties in mapping lessons with different security requirements. This is due to the subjective nature of the GSN, that allows the template to be further reviewed and discussed by others. Chapter 8 uses a focus group study and the participants expressed that the discussion process helped them come to an agreement and better understand the reasoning between the lessons learned and the goals.

9.1.2 Dissertation research question 2

The answer to research question 2 “Can the Generic Security Template better assist users to identify lessons from security incidents by comparing to the traditional pure free text approach?” is yes. In Chapter 5, we have conducted an empirical study with 24 university students from a variety of education backgrounds to evaluate the utility and usability of conventional text-based security incident reports with a graphical formalism based on the Goal Structuring Notation. The two methods were compared in term of the users’ accuracy, efficiency to identify a number of lessons learned (causes of the incident but also the participants’ ability to understand the reasons why particular recommendations were proposed as ways of avoiding future violations) from investigations into previous incidents involving the disclosure of healthcare records, as well as reasoning on security arguments (i.e. the supportive relationships between lessons learned and violated security requirements). Even using a relatively small sample, we were able to obtain statistically significant differences in terms of their accuracy rate in identifying lessons learned from the security incident. The group with the GST perform better than the group with text alone. We are able to obtain statistically significant differences for identifying the relationships between the lessons learned and the security requirements, and the group with template performs better. We are not able to obtain efficiency (time) difference between the two groups. A reason could be it is the first time they used the GST, they have spent sometime to read over through all the text document and the template. However, their subjective feedback revealed they had experienced learning effects. Their confidence in answering the questions increased as they worked their way through the questions, and their overall feedback towards the GST is positive.

9.1.3 Dissertation research question 3

The answer to research question 3 “Can the Generic Security Template be used for feeding back the lessons learned to information security management system (ISMS) in healthcare industry?” is partially yes. In Chapter 6, we conducted a case study with fifteen subjects (five security professionals, ten healthcare professional) working in a Chinese healthcare organisation to study their current security management systems, the incident handling processes, the feedback of the learning to the ISMS, as well as their general attitude and acceptance towards the Generic Security Template. The results show that, lessons are not effectively fed back into the ISMS, which is consistent with the findings in the literature review. In particular they demonstrated their interests in investigating on how lessons identified from the security incidents happened in different countries can be transferred to their organisation to inform the improvements of their Information Security Management Systems.

The above mentioned interviews study with healthcare professionals in China provided initial insights into the application of our approach. In Chapter 8, we look beyond subjective impressions to provide more direct evidence about whether or not security lessons can be transferred between healthcare organisations in different countries. In particular, we used three instances of the Generic Security Template, which are the VA 2006, VA 2007 and Shenzhen data leakage incidents to investigate whether Chinese healthcare professionals could transfer security lessons from those incidents in their own context. The findings show that learning from security incidents in other healthcare organisations both at home and abroad can indeed be transferred into XXX central hospital. We also identified a process for the transferability of lessons learned using the Generic Security Template. This contributes to the sharing of the security incidents and the exchange of security lessons globally. Moreover, other customisation requirements were raised and collected such as the recommendation acceptance identifier and the multi-view identifier. Finally, the Generic Security Template has been customised and improved, which guides the directions for future development.

9.2 Contributions

A novel approach to feed back the lessons learned identified from healthcare security incidents to Information Security Management Systems (ISMS). The Generic Security Template brings together lessons learned from security incidents and maps them to the

security requirements of the ISMS. Those lessons are presented in a structured manner and serve as an additional resource that can add to existing security controls (e.g. the security standards, best practices). It also contributes to the ‘feedback’ or ‘follow-up’ phase of the security incident response lifecycle, as it provides a systematic way to deal with the lessons from security incidents and share them in a structured manner. This has implication in increasing the accessibility of the lessons learned identified from the security incident.

An approach to improve the comprehension of Security Incidents Report. Through an empirical study conducted in this research, we have found that the Generic Security Template can help improving the accuracy and reducing the mental efforts in comprehending the security incident report, and the results are statistically significant. This has implication and contributes to tackling the current frustration faced by the stakeholders who do not have time to read the security incident report. It also enables the security incident report to be more accessible and usable in real practice.

The potential in communicating lessons learned from the security incidents. Through the first industrial evaluation, the Generic Security Template has been found to have the potential to improve the effectiveness in communicating security incidents. Application scenarios have been identified by the participants, to communicate security incidents in team meetings. This finding shows that the Generic Security Template has the potential to contribute to encourage people to speak the same language while communicating security incidents.

Cross-country transfer of lessons learned in healthcare organisations. Through the second healthcare evaluation of the Generic Security Template, we have demonstrated that lessons learned from security incidents can be transferred using the Generic Security Template. This finding shows that the Generic Security Template can contribute to the exchange of security incidents in healthcare organisations from different countries. During this process, the lessons learned from security incidents in different countries are mapped to different levels of the security requirements of the security standard that applies for a different organisation. In addition, the process on the exchange of the lessons learned is also identified in this study, this provide guidance and pave the ways for future work on transferring the lessons learned from the security incident across different healthcare organisations. The transferability of lessons learned increases exposure to the security incident report and create a greater audience, hence enhancing current incident learning practices.

Implications for the Goal Structuring Notations (GSN). The GSN was traditionally

used in presenting safety/ security assurance case. The Generic Security Template is a new application of the GSN by adapting it to satisfy the design requirements of the Generic Security Template. Our empirical work in evaluation of the Generic Security Template also contributed to the evaluation of the GSN since there has not been similar evaluation work found in the security area.

9.3 Limitations and directions for future work

This section discusses several limitations and directions for future work.

9.3.1 Subjective features

Throughout the evaluation of the Generic Security Template, users have identified difficulties due to subjective nature of the approach, especially on the rules to map lessons learned to the goals (security requirements). The healthcare evaluations generated a set of rules that help to decide the mapping in Chapter 6. According to feedback from an empirical study in Chapter 7, it can hardly ensure that users following the rules can have the same results. However, the translation from natural language statements into structured graphical overview is not an automatic process [139]. It requires the analysts' skill and judgement. This is consistent with the subjective nature of the GSN approach itself, which allows people to reason about the arguments between lessons and goals [7]. The industrial evaluation in Chapter 8 uses a focus group study and the participants expressed that the discussion process helped them come to an agreement and better understand the reasoning between the lessons learned and the goals. Future study can focus on a more formalised way and experience can be borrowed from the formalisation of other diagramming approaches such as the Unified Modified Language (UML) [230–233].

The decision of the level of abstraction is a subjective process. The security analysts define their own level of details in the security incident report according to individual business needs. Within this research, a majority of the participants did not concern about the level of details nor suggested any changes to the evaluated cases. However, too much information will undermine the effectiveness of the graphical presentation, while too little information will make it difficult to understand. There are some existing works on model abstraction. For example, Polyvyanyy proposed an abstraction slider to allows user control of the model abstraction level [234]. Smirnov

presented abstraction approach, addressing specific features of BPMN [235]. Future work can focus on model abstraction as well as business intelligence [236–238] to generate lessons learned with a desirable level of details.

9.3.2 Scalability

Based on the feedback from a series of evaluations, the participants raised scalability concerns for the Generic Security Template. This is a common problem with graphical notations. Experience in safety can be borrowed to address this issue. Using the GSN, they break down safety cases into different sub-cases and then link them back to a main case. There are commercial tools available for supporting the creation of the safety cases [239, 240]. Future work can customise these tools to satisfy the needs of the Generic Security Template.

9.3.3 Traceability

As is mentioned, the GST is not intended to replace any of the existing lessons learned dissemination methods, but can serve as a ‘road-map’ over the existing incident report, that removes the burden of communicating potentially complex dependencies within the pure text report. The traceability linking the GST and the textual report can hardly be maintained through manual co-relation. Future work can customise the commercial tools [239, 240] to support this feature.

9.3.4 Soundness

The soundness of the instances created by the Generic Security Template is also a focus of future work. Within safety area, confidence argument has been proposed to answer such question by providing details on completeness of the identified issues, quality, strength and trustworthiness of the evidence, and quality of the development processes [241]. There are also some existing work on applying formalisms to mechanically check the logical soundness of cases [139, 242, 243]. Those will be the focus of future works.

9.3.5 Industrial evaluation

This research has identified the potential benefits for the healthcare organisation to apply this approach over their existing mechanisms through an explorative industrial

case study. However, the results have not been empirically evaluated. Future work should conduct comparative experiment studies to confirm this finding. We performed the study within one healthcare organisation in China. The findings might hardly be generalised into other healthcare organisations in other countries with a different context. However, this provides the basis for future work in conducting the same study in other healthcare organisations.

9.4 Closing remarks

In this dissertation we have proposed the Generic Security Template aiming to feed back lessons learned from the security incidents to ISMS. The empirical study shows that it can help to improve the comprehension of lessons. Healthcare evaluations show that it might help to exchange the lessons learned from the healthcare organisation around the globe to a healthcare organisation in China. During this exchange process, the organisation has considered their own practices and assessed whether applicable security standards within their Information Security Management Systems address the concerns raised in previous breaches. The experience gained within the regime of this PhD provides foundational work to generalise the use of this approach to other industries.

Appendix A

Security Incident Case Studies (Appendix to Chapter 4)

A.1 Veterans Affairs (VA) data leakage incident 2006

Table A.1: Veterans Affairs (VA) data loss incident 2006

Security Issues	Security Recommendations
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage
Position Description	Define the position sensitive level.
Security Training	Provide linkage to all applicable laws and VA policy as part of the security awareness training.
Incident Handling	Enhance incident-response program for promptly identification and thoroughly investigation of the incidents.
Administrative Action	Take appropriate administrative action against the people involved in this incident for their inappropriate actions.

A.2 Veterans Affairs (VA) data leakage incident 2007

Table A.2: Veterans Affairs (VA) dataloss incident 2007

Security Issues	Security Recommendations
Access Control	Avoid the abuse of programmer level access control.
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage
Security Policy	Ensure that data security plans for research projects comply with information security policies.
Security Policy	Ensure human subjects in research, compliance with information security requirements.
Security Policy	Discontinue storing email on unauthorized system.
Position Description	Re-evaluate and correct position sensitivity levels.
Management Structure	Establish a functional description and performance plan to clarify the line authority and reporting relationship.
Administrative Action	Take appropriate administrative actions against the people for their inappropriate actions.
Risk Analysis	Develop and issue Government-wide risk analysis criteria.

A.3 Shenzhen data leakage incident 2008

Table A.3: Shenzhen dataloss incident 2008

Security Issues	Security Recommendations
Network Security	Network security needs to be ensured by following the security standards.
Sensitive Information	Define the information sensitive level according to the security standards.
Security Policy	Establish and enforce security policy according to the security standards.
Security Audit	Establish and conduct security audit plan according to the security standards.
Security Training	Establish and execute security training programs by following the security standards.

A.4 NHS Surrey IT Asset Disposal Incident 2013

Table A.4: NHS Surrey IT Asset Disposal Incident 2013

Security Issues	Security Recommendations
Risk Management	Carry out a risk assessment when using a data processor to dispose of the hard drives.
Personal Data	Wipe medical information and confidential sensitive data before recycling.
Contract	Have a written contract with the company processing the IT Asset.
Disposal Monitoring	Monitor the destruction process and maintain audit trails and inventory logs of hard drives destroyed by the company based on the serial numbers in the destruction certificates for each individual drive.
Remedial Action	Take remedial action which includes developing a new policy framework to address the internal re-use of information and appliances and disposal process for redundant equipment.

A.5 Security incidents in the US, China and UK

Security Incidents in the US

1. Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans

<http://www.va.gov/oig/pubs/VAOIG-06-02238-163.pdf>

2. Administrative Investigation Loss of VA Information VA Medical Centre Birmingham, AL

<http://www.va.gov/oig/pubs/VAOIG-07-01083-157.pdf>

3. Review of Alleged Unauthorized Access to VA Systems

<http://www.va.gov/oig/52/reports/2011/VAOIG-10-03516-229.pdf>

4. Review of Alleged Mismanagement of the Systems to Drive Performance Project

<http://www.va.gov/oig/pubs/VAOIG-11-02467-87.pdf>

5. Review of Information Security Issues Impacting VA Teleradiology Contracts

<http://www.va.gov/oig/52/reports/2010/VAOIG-09-03122-198.pdf>

6. Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

<http://www.va.gov/oig/pubs/VAOIG-12-02802-111.pdf>

Security Incidents in China

1. 深圳 10 万孕产妇个人信息遭泄露
<http://news.sina.com.cn/s/2008-06-10/020715710408.shtml>
2. 黑客伪造 WiFi 热点盗取个人信息
<http://tech.sina.com.cn/t/2012-02-25/04196767784.shtml>
3. 程序员入侵证券公司导致 40 万条股民信息泄漏
<http://finance.ifeng.com/stock/tzgs/20120420/5968175.shtml>
4. 黑客攻破中电信网络盗取 900 个内部管理账户
<http://tech.163.com/12/0604/14/835LP3N8000915BE.html>
5. 黑客入侵政府、大学网站添加虚假信息倒卖上万假证
http://edu.ifeng.com/gaoxiao/detail_2012_07/26/16323038_0.shtml
6. 因信号系统受干扰 深圳地铁发生暂停故障
<http://tech.sina.com.cn/t/2012-11-16/01577802256.shtml>
7. 空调故障导致 12306 网站三天内两次瘫痪
<http://sh.eastday.com/m/20121227/u1a7091836.html>
8. 上千万台计算机被盗取 QQ 及 Q 币
<http://it.sohu.com/20120515/n343205468.shtml>
9. 安全漏洞导致上千万银行卡客户信息泄露
<http://finance.ifeng.com/bank/yhk/20120401/5854381.shtml>
10. 黑客攻击 DNS 操控电脑净赚 1400 万美元
<http://news.sina.com.cn/w/2012-04-23/174624316823.shtml>
11. 警方破获特大网银盗窃案 近百人被盗千万
<http://finance.ifeng.com/roll/20120808/6888882.shtml>
12. 亚马逊中国账户大规模被盗 涉及用户或超千人
<http://it.sohu.com/20120907/n352615210.shtml>
13. 超 10 万个假冒、钓鱼网站被处理
http://news.xinhuanet.com/2010-12/17/c_12889639.htm

Security Incidents in UK

1. Councils fined for serious data breaches

http://ico.org.uk/news/latest_news/2012/councils-fined-for-serious-data-breaches-13022012

2. British Pregnancy Advice Service fined £200,000

http://ico.org.uk/news/latest_news/2014/british-pregnancy-advice-service-fined-200000-07032014

3. ICO fines Glasgow City Council £150K

http://ico.org.uk/news/latest_news/2013/Glasgow-city-council-fined-150000-07062013

http://ico.org.uk/news/latest_news/2013/~media/documents/library/Data_Protection/Notices/Glasgow-city-council-monetary-penalty-notice.ashx

4. Council fined for serious email disclosure

http://ico.org.uk/news/latest_news/2012/council-fined-for-serious-email-disclosure-15022012

5. NHS Trust fined £325,000 following data breach affecting thousands of patients and staff

http://ico.org.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012

6. Telford and Wrekin Council fined £90,000 following disclosure of vulnerable children's data

http://ico.org.uk/news/latest_news/2012/telford-wrekin-council-fined-following-disclosure-of-vulnerable-childrens-data-06062012

7. Council fined £70,000 for losing highly sensitive data

http://ico.org.uk/news/latest_news/2012/council-fined-70000-for-losing-highly-sensitive-data-16052012

8. Repeated security failings lead to £180,000 fine for Ministry of Justice

http://ico.org.uk/news/latest_news/2014/repeated-security-failings-lead-to-180000-fine-for-moj-26082014

9. ICO fines NHS Surrey for failing to check the destruction of old computers

http://ico.org.uk/news/latest_news/2013/~media/documents/library/Data_Protection/Notices/nhs-surrey-monetary-penalty-notice.pdf

http://ico.org.uk/news/latest_news/2013/ico-issues-nhs-surrey-monetary-penalty-of-200000

10. Pay day loans company fined £175,000 over millions of spam texts
http://ico.org.uk/news/latest_news/2013/payday-loans-company-receives-175000-fine-over-spam-texts

11. London NHS Trust fined £90,000 for serious data breach
http://ico.org.uk/news/latest_news/2012/london-nhs-trust-fined-90000-for-serious-data-breach-21052012

12. Sony fined £250,000 after millions of UK gamers' details compromised
http://ico.org.uk/news/latest_news/2013/ico-news-release-2013
http://ico.org.uk/news/latest_news/2013/~media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx

13. Belfast Trust fined £225,000 after leaving thousands of patient records in disused hospital
http://ico.org.uk/news/latest_news/2012/belfast-trust-fined-225000-after-leaving-thousands-of-patient-records-in-disused-hospital-19062012

14. Sensitive details of NHS staff published by Trust in Devon
http://ico.org.uk/news/latest_news/2012/sensitive-details-of-nhs-staff-published-by-devon-trust-06082012

Appendix B

The Empirical Experiment (Appendix to Chapter 5)

B.1 Participant Consent Form: Usability of GST

The objective of the experiment is to assess the usability of “Generic Security Template” in terms of the Accuracy and Efficiency to assist comprehending security incidents and its Ease of use by comparing to the Text-based approach.

INFORMATION

The experiment was a paper-based exercise, which was conducted in a one hour slot. The steps include: (1) Familiarisation with Generic Security Template by a Tutorial Session; (2) Completion of experiment tasks, which is to comprehend security incident report with/without the help of Generic Security Template and answer a few questions related to the given security incident sample. (3) Filling-out of a post-experiment questionnaire.

RISKS

The risks associated in this experiment might be slightly strains as it is a bit mentally demanded.

CONFIDENTIALITY

The information of this experiment including participant’s response record, experiment data will be kept confidential and can only be accessed by this research conductor. No reference will be made in any report, which may link the participants to the study.

PARTICIPATION

Your participation in this study is voluntary. If you decide to participate, you may withdraw at any time without penalty.

CONTACT

If you have questions about the study, please contact:

Miss Ying He, Email: yingh@dcs.gla.ac.uk

Prof Chris Johnson, Email: Christopher.Johnson@glasgow.ac.uk

School of Computing Science, University of Glasgow

DECLARATION

“I confirm that I have read and understand the information above. I agree to participate in this study with the understanding that I may withdraw at any time.”

Signed

Date

Contact Information

This study adheres to the BPS ethical guidelines, and has been approved by the FIMS ethics committee of The University of Glasgow (ref: CSE01098).

B.2 VA Data Leakage Incident 2007

VA's Data Loss Incident 2007

On January 22, 2007, a Veterans Health Administration (VHA) Information Technology (IT) Specialist assigned to the Research Enhancement Award Program (Birmingham REAP), VA Medical Centre (VAMC), Birmingham, AL, reported that a VA-owned external hard drive was missing from the REAP office. The missing external hard drive was believed to contain numerous research-related files containing personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the Centres for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS), on over 1.3 million medical providers. Investigation conducted to identify the problem and recommendations were provided by VA office of Inspector General.

Problem Identified

Issue 1: Circumstances Surrounding How the Data Went Missing, the Extent and Magnitude of the Data Loss, and Whether VA Appropriately Responded to the Incident.

Notifications of data loss to VAMC Information Security Officer (ISO), VA Management and Office of Inspector General (OIG) were both Timely and appropriate. A criminal investigation is opened immediately in determining how data went missing. The Initial Notification of Magnitude of the Dataloss was Inaccurate because the IT Specialist encrypted and/or deleted multiple files from his computer shortly after he reported the data missing in an attempt to hide the extent, magnitude, and impact of the missing data.

VA began sending notification letters informing each recipient that one of the files on the portable hard drive may have contained the recipients' name, SSN, DOB, and health information, offering them the option of 1 year of free credit monitoring services. This data loss comes from more than one Federal Agencies and it raises concerns over the need for Government-wide Criteria for Assessing Risk Associated with Data Loss on what constitutes high risk data for identity theft.

Issue 2 Whether There Were Policies, Procedures, and Controls in Place to Properly Store and Safeguard the Missing Data.

Birmingham REAP Managers Did Not Ensure Proper Information Security Controls to Safeguard Data Stored on External Hard Drives. There was no VA policy in effect at the time the external hard drive went missing that addressed the need to protect sensitive data on removable computer storage devices, unless those devices were carried outside a VA facility. Although VISN 7 policy required encryption on these devices, the Birmingham REAP Director did not request encryption software.

Position Sensitivity Level Assessments were Not Adequately Performed. The position sensitivity level for the IT Specialist was inaccurately designated as moderate risk, which was inconsistent with his programmer privileges and resulted in a less extensive background investigation.

Issue 3 Whether the IT Specialist was Appropriately Authorized Access to Large Amounts of Protected Information.

The IT Specialist was improperly given access to multiple data sources, allowing him to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects. Three research projects involved in this dataloss were evaluated and here are the findings.

VISN 7 officials improperly gave the IT Specialist access to data from the VISN Data Warehouse that contained scrambled SSNs (known as SCRSSNS), which are considered to be personally identifiable information. The IT Specialist was also given programmer level access to VistA (Veterans Health Information Systems and Technology Architecture) at Birmingham without sufficient authorization.

The Birmingham REAP Data Security Plan did not comply with the VISN 7 policy or VIREC guidance, the approval by the IRB committee, the R&D Committee, and the Medical Center Director's Office was inappropriate and resulted in VIREC's release of the data even though the REAP did not have adequate procedures to protect the security of the data.

The IT Specialist was essentially given unfettered access to several files maintained by the VA Austin Automation Center (AAC), Austin, TX, even though the requests were not appropriately authorized. The IT Specialist's access to these files did not comply with VHA policy or the Privacy Act.

Issue 4 Whether the IT Specialist Complied with Research Project Protocols to Properly Safeguard Protected Information.

The IT Specialist violated the terms and conditions under which the IRB granted HIPAA waivers for the involved protocols. In doing so, the IT Specialist failed to properly safeguard individually identifiable health information, thereby placing vast amounts of HIPAA and Privacy Act protected information at risk.

Issue 5 Whether the Birmingham REAP Director Was Adequately Supervised, and Whether the REAP's Director and Associate Director Adequately Managed and Supervised the Operations and Staff of the REAP.

The REAP Director and her subordinate managers frequently were not physically present at the REAP to supervise and manage daily operations. She had her official VA e-mail automatically forwarded to her account at the University of Alabama, in violation of VA policy. The REAP Director's supervisor of record, the ACOS for Acute and Specialty Care, in fact, was the supervisor in name only and provided no supervision. The Associate Chief of Staff for Research, though responsible for all research programs at the Birmingham VAMC, has no line authority over the REAP and did not supervise the REAP Director. While the Medical Centre Director is ultimately responsible for position management at the facility, he also did not ensure adequate supervision over REAP operations.

Recommendations

Issue 1:

Recommendation (1): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for his inappropriate actions during the course of the investigation and for failing to properly safeguard personally identifiable information on his missing external hard drive.

Recommendation (2): We recommend that the Assistant Secretary for Information and Technology coordinate with the Office of Management and Budget and the President's Identity Theft Task Force to develop and issue Government-wide risk analysis criteria to determine under what conditions potential identity theft victims should be notified and offered free credit monitoring. In the interim, the Assistant Secretary for Information and Technology should re-evaluate VA policy to determine whether the loss of a solo personal identifier, such as a social security number only, would constitute a risk for identity theft for purposes of offering free credit monitoring.

Issue 2:

Recommendation (3): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham REAP Director and Associate Director for failing to take adequate security measures to protect personally identifiable information.

Recommendation (4): We recommend that the Assistant Secretary for Information and Technology revise VA Directive 6601 to require the use of encryption, or an otherwise effective tool, to properly protect personally identifiable information and other sensitive data stored on removable storage devices when used within VA.

Recommendation (5): We recommend that the Under Secretary for Health direct the Medical Center Director to re-evaluate and correct position sensitivity levels and associated background investigations for positions at the Birmingham VAMC.

Issue 3:

Recommendation (6): We recommend that the Under Secretary for Health develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information from VISN data warehouses for research purposes to include IRB approval requirements and stress, in VHA's mandatory annual privacy training, that scrambled SSNs do not constitute de-identified data.

Recommendation (7): We recommend that the Assistant Secretary for Information and Technology develop and implement policies describing the conditions under which VistA programmer level access may be granted for research purposes, including whether that access is project specific or for the term of employment, and take appropriate action to remove programmer access from individuals who do not meet those conditions.

Recommendation (8): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the MAC and VIREC Directors for inappropriately retaining and releasing the MPIER file.

Recommendation (9): We recommend that the Under Secretary for Health develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval by the IRB.

Recommendation (10): We recommend that the Assistant Secretary for Information and Technology disseminate and enforce the existing Standard Operating Procedure for access to Austin Automation Center's nationwide SSN file, and issue policies and procedures regarding authorization to access all other Austin Automation Center data for research purposes.

Issue 4:

Recommendation (11): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for inappropriately accessing and utilizing individually identifiable health information.

Recommendation (12): We recommend that the Under Secretary for Health require facility IRB compliance program audits to assess the privacy and confidentiality protections for human subjects in research, including whether the use of research data complies with information security requirements specified in HIPAA waivers or waivers of informed consent.

Issue 5:

Recommendation (13): We recommend that the Under Secretary for Health ensure that the Birmingham REAP Director and Associate Director discontinue the practice of receiving their official VA e-mail at the University of Birmingham, in violation of VA policy prohibiting storage of VA information on a non-VA system, resulting in potential Privacy Act or HIPAA violations.

Recommendation (14): We recommend that the Under Secretary for Health assess the alignment of Birmingham REAP management positions at the Birmingham VAMC, and take action to correct the dysfunctional management structure that led to an overall breakdown of management oversight, controls, and accountability of the Birmingham REAP. This should include:

- Correction of the Birmingham REAP Director's reporting relationship from the ACOS for Acute and Specialty Care, which was in name only and resulted in the lack of actual supervision over the REAP Director's activities, to the ACOS for Research who currently has facility-wide responsibility for research programs but no line authority over REAP managers or involvement in their activities.
- Establishment of an accurate functional description and performance plan to clarify Birmingham REAP managers' responsibilities and to hold them accountable for proper administration of REAP resources, to include equipment purchases, acquisition of server space, protection of sensitive information stored on VA systems and portable devices, office space security, and compliance with applicable VA policies and procedures.
- Clarification of the Medical Center Director and ACOS for Research's responsibility and line authority over all research programs at the facility, including the Birmingham REAP.

Recommendation (15): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham Medical Center Director for not ensuring appropriate management and administration of the Birmingham REAP and protection of the privacy and confidentiality of research subjects.

Recommendation (16): We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the ACOS for Research for not ensuring appropriate management and administration of the Birmingham REAP.

B.3 Security Standards

SM: Security management is controlled

SM 1. Security management program is established.

SM 1.1. The security management program is adequately documented, approved, and up-to-date.	SM 1.1.1. An agency/entity-wide security management program has been developed, documented, and implemented. SM-1.1.2. The agency/entity-wide security management program is updated to reflect current conditions.
SM 1.2: A security management structure has been established.	SM 1.2.1. Senior management establishes a security management structure for entity-wide, system, and application levels that have adequate independence, authority, expertise, and resources. SM 1.2.2. An information systems security manager has been appointed at an agency/entity level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority.
SM-1.3. Information security responsibilities are clearly assigned.	SM-1.3.1. The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined at the entity-wide, system, and application levels.
SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date.	SM-1.4.1. System and application security plans have been documented and implemented SM-1.4.2. The subordinate security plans is updated annually or whenever there are significant changes to the agency/entity policies, organization, IT systems, facilities, applications, weaknesses identified, or other conditions that may affect security.
SM-1.5. An inventory of systems is developed, documented, and kept up-to-date.	SM-1.5.1. A complete, accurate, and up-to-date inventory exists for all major systems that includes the identification of all system interfaces.

SM 2. Periodically assess and validate risks

SM-2.1. Risk assessments and supporting activities are systematically conducted.	SM-2.1.1. Appropriate risk assessment policies and procedures are documented and based on security categorizations. SM-2.1.2. Information systems are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals. SM-2.1.3. Risks are reassessed for the entity-wide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change. SM-2.1.4. Risk assessments and validations, and related management approvals are documented and maintained on file. Such documentation includes security plans, risk assessments, security test and evaluation results, and appropriate management approvals. SM-2.1.5. Changes to systems, facilities, or other conditions and identified security vulnerabilities are analysed to determine their impact on risk and the risk assessment is performed or revised as necessary based on OMB criteria.
--	---

SM 3. Security control policies and procedures are documented and implemented.

SM-3.1 Security control policies and procedures are documented, approved by management and implemented.	SM-3.1.1. Security control policies and procedures at all levels, <ul style="list-style-type: none">• are documented,• appropriately consider risk,• address purpose, scope, roles, responsibilities, and compliance,• ensure that users can be held accountable for their actions,• appropriately consider general and application controls,• are approved by management, and• are periodically reviewed and updated.
---	--

AC: User access control is addressed

AC 3. Effective authorization controls are implemented

AC 3.1. User accounts are appropriately controlled.	AC 3.1.1. Resource owners have identified authorized users and the access they are authorized to have. AC 3.1.2. Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs.
AC 3.2. Processes and services are adequately controlled.	AC 3.2.1. Available processes and services are minimized, such as through, <ul style="list-style-type: none">• installing only required processes and services based on least functionality,• Restricting the number of individuals with access to such services based on least privilege,• monitoring the use of such services, and• maintaining current service versions. AC-3.2.2. The function and purpose of processes and services are documented and approved by management.

AC 4: Sensitive system resources are adequately protected.

AC 4.1: Access to sensitive system resources is restricted and monitored.	AC 4.1.1. Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose. AC 4.1.2. Use of sensitive/privileged accounts is adequately monitored.
---	---

AC 5: An effective audit and monitoring capabilities is implemented.

AC-5.1. An effective incident response program is documented and approved.	AC-5.1.1. An effective incident-response program has been implemented and include <ul style="list-style-type: none">• documented policies, procedures, and plans;• documented testing of the incident response plan and follow-up on findings;• a means of prompt centralized reporting;• active monitoring of alerts/advisories;• response team members with the necessary knowledge, skills, and abilities;
--	---

	<ul style="list-style-type: none"> • training on roles and responsibilities and periodic refresher training; • links to other relevant groups; • protection against denial-of-service attacks (see http://icat.nist.gov); • appropriate incident-response assistance; and • consideration of computer forensics.
AC-5.2. Incidents are effectively identified and logged.	<p>AC-5.2.1. An effective intrusion detection system has been implemented, including appropriate placement of intrusion-detection sensors and incident thresholds.</p> <p>AC-5.2.2. An effective process has been established based on a risk assessment, to identify auditable events that will be logged.</p> <p>AC-5.2.3. All auditable events, including access to and modifications of sensitive or critical system resources, are logged.</p> <p>AC-5.2.4. Audit records contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred (for example, time stamps), the source of the events, and the outcome of the events.</p>
AC 5.3. Incidents are properly analysed and appropriate actions taken.	<p>AC 5.3.1. Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported and investigated.</p> <p>AC 5.3.2. Security managers investigate security violations and suspicious activities and report results to appropriate supervisory and management personnel.</p> <p>AC 5.3.3. Appropriate disciplinary actions are taken.</p>

B.4 Experiment Description

Experiment Material

1. Security Incident Report (Textual Description)

VA 2007 Data Loss Incident Report - Appendix B.2, and B.3

2. Instance of the Generic Security Template (Diagram Description)

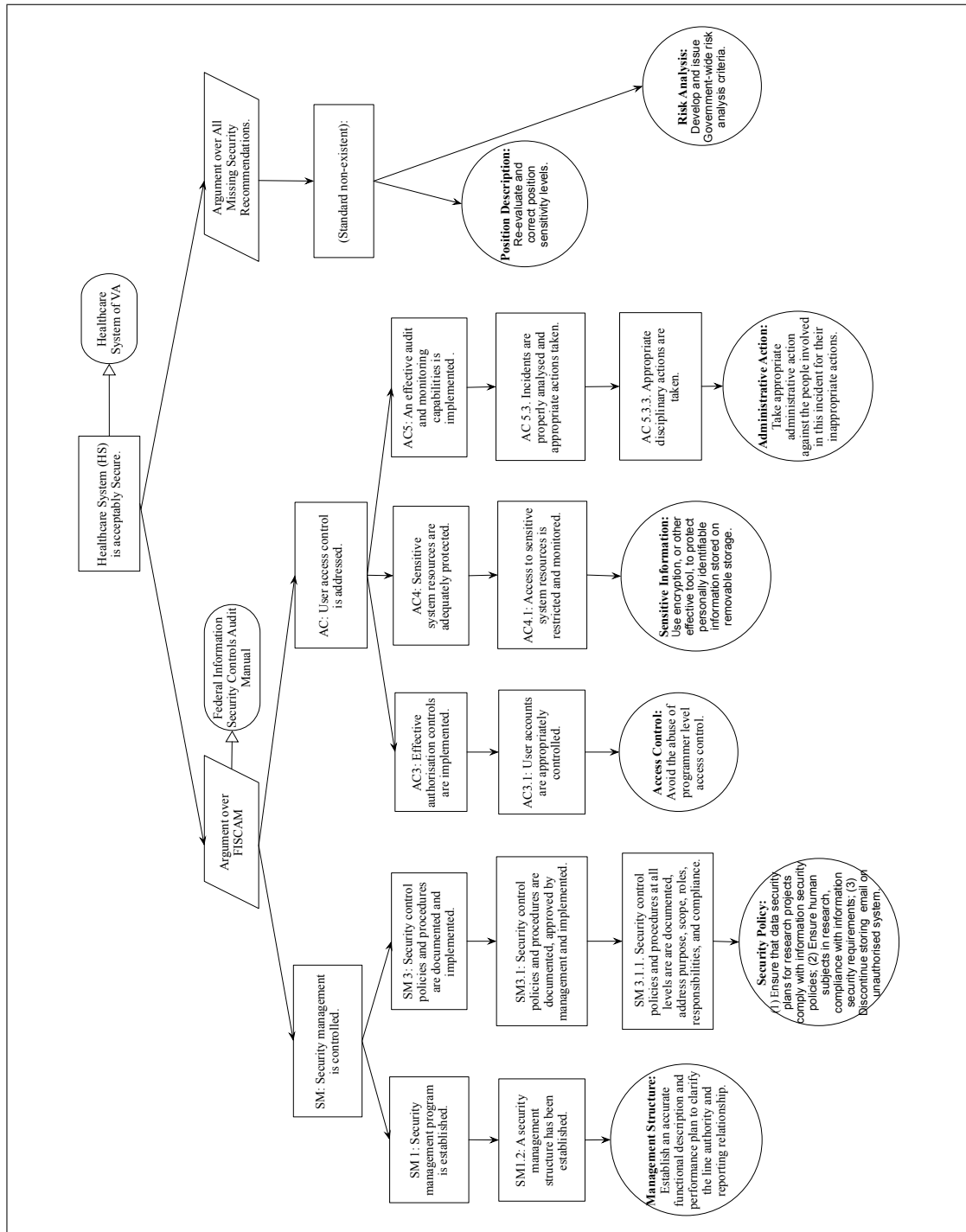


Figure B.1: Generic Security Template - VA data leakage 2007

B.5 Experiment Tasks

Task 1 Security Lessons Identification

Identify the Security Issues and Recommendations from the given text based report with the help of the “Generic Security Template” and fill in the table below,

Issue Category	Issue description	Recommendations description
<i>Risk analysis Related</i>	Data loss comes from more than one Federal Agencies and it raises concerns over the need for Government-wide Criteria for Assessing Risk Associated with Data Loss on what constitutes high risk data for identity theft.	
<i>Position Description Related</i>		Re-evaluate and correct position sensitivity levels and associated background investigations for positions.
<i>Access Control Related</i>	The IT Specialist was improperly given access to multiple data sources.	
<i>Security Policy Related</i>		develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information; develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval.

Table B.1: Experiment task 1

<i>Security Policy Related</i>	Violation of the terms and conditions under granted HIPAA waivers for the involved protocols. Failure to properly safeguard individually identifiable health information	
<i>Security Policy Related</i>		Discontinue the practice of receiving their official VA e-mail and storing VA information on a non-VA system.
<i>Management Structure Related</i>	Dysfunctional management structure which was not adequately supervised is likely to lead to an overall breakdown of management oversight, controls, and accountability of the organization.	
<i>Administrative Actions Related</i>	People's inappropriate actions during the course of the investigation and for failing to take adequate security measures to protect personally identifiable information and for not ensuring appropriate management and administration of the organization.	Appropriate administrative action needs to be taken against the people involved in this incident for their inappropriate actions during the course of the investigation and for failing to take adequate security measures to protect personally identifiable information and for not ensuring appropriate management and administration of the organization.

Table B.2: Experiment task 1 (continued)

Task 2 - Relationships Identification.

There are one or more options that are correct for the questions. Circle the options of the correct answers.

1. The Security Recommendations of the Security Incident are to address the following security objectives.
 - a. Access Control
 - b. Security Control Policy and Procedure
 - c. Security Management Program
 - d. Sensitive Information Management
 - e. Security Management Structure and Procedure
 - f. Security Awareness Training
 - g. System Configuration
 - h. Change Management
 - i. Security Incident Handling Process
 - j. None of the above

2. The recommendations on “Security Structure Management” are
 - a. Security Incidents needs to be responded timely.
 - b. The establishment of an accurate functional description and performance plan to clarify managers’ responsibilities,
 - c. The clarification of reporting relationship and line authority over all research programs.
 - d. None of the above

3. What are the security recommendations for addressing the security objective “User Access Control”
 - a. Develop and implement policies describing the conditions under which programmer level access may be granted for research purposes
 - b. Effective procedures are implemented to determine compliance with authentication policies.
 - c. Attempts to log on with invalid passwords are limited. Use of easily guessed passwords (such as names or words) is prohibited.
 - d. None of the above

4. What are the security recommendations for addressing the security objective “System Configuration”

- a. System Configuration policies, plans and procedures have been developed, documented, and implemented
- b. Configuration changes are authorised by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.
- c. Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.
- d. None of the above

5. The recommendation “The use of encryption or an otherwise effective tool to properly protect personal identifiable information” are provided to support the security objectives

- a. Risk assessments and supporting activities are systematically conducted.
- b. Access to sensitive system resources is restricted and monitored.
- c. User Access Control is sufficiently addressed
- d. None of the above

6. The recommendation “the establishment of an accurate functional description and performance plan to clarify manager’s responsibility” are provided to support the security objectives

- a. Security control policies and procedures are documented, approved by management and implemented
- b. Security management program is successfully established
- c. Security management structure has been established
- d. None of the above

1. How mentally demanding was the task?

Low □□□□□□□□□□□□□□□□ High
2. How hurried or rushed was the pace of the task?

Low □□□□□□□□□□□□□□□□ High
3. How discouraged, stressed, and annoyed did you feel when doing the tasks?

Low □□□□□□□□□□□□□□□□ High
4. How successful do you feel in accomplishing the task?

Low □□□□□□□□□□□□□□□□ High
5. How hard did you have to work to complete the task?

Low □□□□□□□□□□□□□□□□ High

Section C: Usability Evaluation Framework Cognitive Dimensions(CD) of Generic Security Template

6. (Visibility) It is easy to see or find the various parts of the Generic Security Template while it is being used?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain what kind of things is difficult to see or find.

7. (Diffuseness) The Generic Security Template let you say what you want reasonably brief?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain what sorts of things take more space to describe.

8. (Hard Mental Operations) There seem some things especially complex or difficult to understand in your head while using the Generic Security Template?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain what are the things.

9. (Closeness of Mapping) The Generic Security Template describes the problem accurately and completely on the security incident stated in Textual Document?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain which parts seem to be a particularly strange way of describing something. Why?

10. (Consistency) There are places where some things ought to be similar, but the Generic Security Template makes them different?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

11. (Role Expressiveness) While reading the Generic Security Template, it is easy to tell what each part is for in the overall scheme?

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Explain which are the things you really don't know what they mean. What are they?

Section D: Participants' experience with the Generic Security Template

12. I have no difficulty in understanding the Security Incident Report (Textual Description).

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

13. I have no difficulty in understanding the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

14. I have no difficulty in identifying Security Lessons (Filling in the table in Task 1) with the help of the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

15. I have no difficulty in identifying Relationships (Answering the multi-choice questions in Task 2) with the help of the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

16. The Generic Security Template helped me better comprehend the security incident by identifying security issues and solutions faster and with less effort than the provided Security Incident Report.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

17. I find it necessary to have the Generic Security Template complimented with correspondent Security Incident Report for better understanding.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

18. I am confident that I can use the Generic Security Template adroitly if I am asked to use it again.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

19. I am satisfied with the overall experience with the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

20. (Open Question) After completing this questionnaire, can you think of obvious ways that the design of the Generic Security Template could be improved? What are they?

B.7 Sample Answer

Task 1 Security Lessons Identification

Identify the Security Issues and Recommendations from the given text based report with the help of the “Generic Security Template” and fill in the table below,

Issue Category ↗	Issue description ↗	Recommendations description ↗
Risk analysis <i>Related</i> ↗	Data loss comes from more than one Federal Agencies and it raises concerns over the need for Government-wide Criteria for Assessing Risk Associated with Data Loss on what constitutes high risk data for identity theft. ↗	<u>Develop and issue Government-wide risk analysis criteria for notifying potential victims with compensation.</u> ↗
Position Description <i>Related</i> ↗	<u>Position sensitivity level assessments were not adequately performed.</u> ↗	Re-evaluate and correct position sensitivity levels and associated background investigations for positions. ↗
Access Control <i>Related</i> ↗	The IT Specialist was improperly given access to multiple data sources. ↗	<u>Develop and implement policies describing the conditions on programmer level access specifying the project and the term and to remove access from individuals who do not meet those conditions.</u> ↗
Security Policy <i>Related</i> ↗	<u>Data security plan was not designed in compliance with security policy.</u> ↗	develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information ; develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval. ↗

Table B.3: Experiment task 1 answer

Security Policy Related ↗	Violation of the terms and conditions under granted HIPAA waivers for the involved protocols. Failure to properly safeguard individually identifiable health information ↗	Human Subjects should be considered in compliance with the security requirement of HIPAA. ↗
Security Policy Related ↗	The REAP director had her official VA e-mail automatically forwarded to her account at the University of Alabama, in violation of VA policy. ↗	Discontinue the practice of receiving their official VA e-mail and storing VA information on a non-VA system. ↗
Management Structure Related ↗	Dysfunctional management structure which was not adequately supervised is likely to lead to an overall breakdown of management oversight, controls, and accountability of the organization. ↗	Correct the dysfunctional management structure that led to an overall breakdown of management oversight, controls, and accountability. ↗
Administrative Actions Related ↗	People's inappropriate actions during the course of the investigation and for failing to take adequate security measures to protect personally identifiable information and for not ensuring appropriate management and administration of the organization. ↗	Appropriate administrative action needs to be taken against the people involved in this incident for their inappropriate actions during the course of the investigation and for failing to take adequate security measures to protect personally identifiable information and for not ensuring appropriate management and administration of the organization. ↗
Sensitive Information Related ↗	Failed to utilise encryption software to protect sensitive data stored on external hard drives. ↗	Encryption or other effective tools need to be applied to protect sensitive information such as personally identifiable information. ↗

Table B.4: Experiment task 1 answer (continued)

Task 2 - Relationships (Security Recommendation and Higher Level Objectives) Identification.

There are one or more options that are correct for the questions. Circle the options of the correct answers.

1. The Security Recommendations of the Security Incident are to address the following security objectives.

- a. Access Control**
- b. Security Control Policy and Procedure**
- c. Security Management Program
- d. Sensitive Information Management**
- e. Security Management Structure and Procedure**
- f. Security Awareness Training
- g. System Configuration
- h. Change Management
- i. Security Incident Handling Process
- j. None of the above

2. The recommendations on “Security Structure Management” are

- a. Security Incidents needs to be responded timely.
- b. The establishment of an accurate functional description and performance plan to clarify managers’ responsibilities**
- c. The clarification of reporting relationship and line authority over all research programs.
- d. None of the above

3. What are the security recommendations for addressing the security objective “User Access Control”

- a. Develop and implement policies describing the conditions under which programmer level access may be granted for research purposes.**
- b. Effective procedures are implemented to determine compliance with authentication policies.**
- c. Attempts to log on with invalid passwords are limited. Use of easily guessed passwords (such as names or words) is prohibited.

- d. None of the above
4. What are the security recommendations for addressing the security objective “System Configuration”
- a. System Configuration policies, plans and procedures have been developed, documented, and implemented
 - b. Configuration changes are authorised by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.
 - c. Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.
 - d. None of the above.**
5. The recommendation “The use of encryption or an otherwise effective tool to properly protect personal identifiable information” are provided to support the security objectives
- a. Risk assessments and supporting activities are systematically conducted.
 - b. Access to sensitive system resources is restricted and monitored.**
 - c. User Access Control is sufficiently addressed.**
 - d. None of the above
6. The recommendation “the establishment of an accurate functional description and performance plan to clarify manager’s responsibility” are provided to support the security objectives
- a. Security control policies and procedures are documented, approved by management and implemented.**
 - b. Security management program is successfully established.
 - c. Security management structure has been established.**
 - d. None of the above.

Appendix C

Industrial Evaluation (Appendix to Chapter 6)

C.1 Participant Consent Form: Acceptance of GST

This research proposes a new incident reporting approach, the Generic Security Template, which we believe can enhance the existing process and the effectiveness in learning the lessons and preventing security incidents.

INFORMATION

The study will be conducted in less than one hour's slot. The steps include: (1) filling-out of a background questionnaire; (2) answer a few questions about current information security management and incident learning in the host organisation; (3) study a real information security incident using the Generic Security Template and provide feedback.

BENIFITS

The benefit you get from this experiment might be (1) the study of a real world security incident; (2) a few recommendations on how to prevent security incident; (3) familiarisation with a graphical incident reporting technique.

CONFIDENTIALITY

All information collected during this study, including the participant's demographic information, and audio records will be kept strictly confidential; This data might be used as part of research publications and reports in journals, conferences and workshops. However, all reported data will be anonymised and all efforts will be undertaken to prevent participants from being identified.

PARTICIPATION

Your participation in this study is voluntary. If you decide to participate, you may withdraw at any time without penalty.

CONTACT

If you have questions about the study, please contact:

Miss Ying He, Email: yingh@dcs.gla.ac.uk

Prof Chris Johnson, Email: Christopher.Johnson@glasgow.ac.uk

School of Computing Science, University of Glasgow

DECLARATION

I confirm that I have read and understand the information above. I agree to participate in this study with the understanding that I may withdraw at any time.

Signed

Date

Contact Information

This study adheres to the BPS ethical guidelines, and has been approved by the FIMS ethics committee of The University of Glasgow (CSE01243).

C.2 Background Questionnaire

Basic Information

Job position (if applicable) _____ Years of experience in this position _____

Highest level of degree _____ Major subject _____

Gender ☐ Male ☐ Female

1. Experience with diagramming technique?

- ☐ Goal Structuring Notations (GSN)
- ☐ Entity-Relationship (ER)
- ☐ Unified Modeling Language (UML)
- ☐ Others, please specify _____

2. Have you read security incident report (e.g. official advert event report)?

☐ Yes

On average, how often do you read them?

A. once a week B. once a month C. once a year D. others, please specify _____

When reading security incident reports I can understand them completely.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

☐ No

3. Have you been involved in security incident handling process?

☐ Yes

Being part of incident handling increased my understanding of the incident.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

☐ No

4. Have you read security standards (such as GB/T22239, etc) in the organization?

☐ Yes

I find security standards helpful in preventing security incidents.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

☐ No

C.3 Tutorial - VA Data Leakage Incident 2007

Generic Security Template

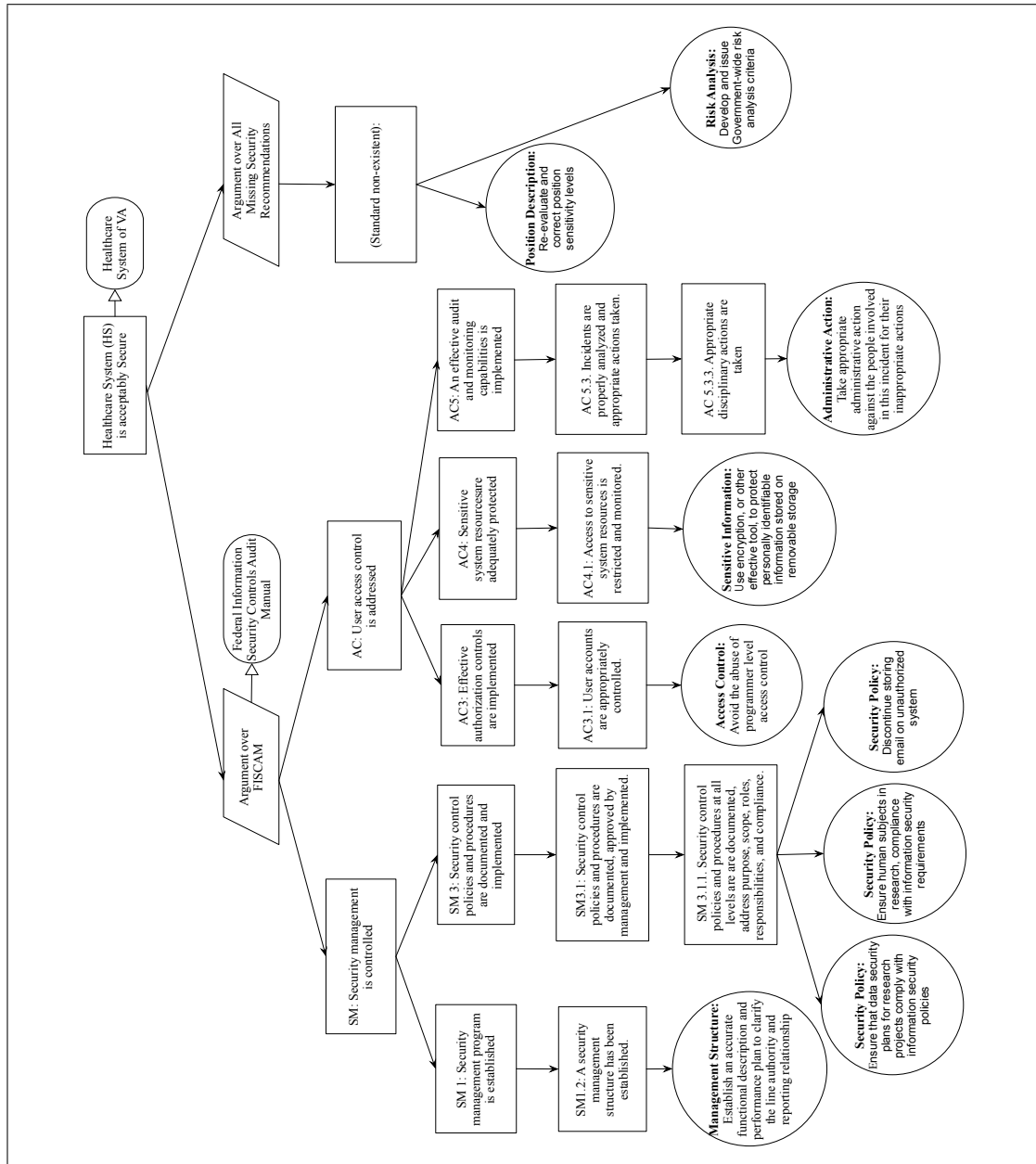


Figure C.1: Generic Security Template - VA data leakage 2007

C.4 Interview Questions

Theme One: The general information security management context.

1. Describe the management support in terms of their support of security training, and encouragement to the organization to learn about information security, or any activities taken to strength the security management.
2. Describe the security culture in terms of how the organization value security, whether the organization promote good security practice, whether their coworkers and management are concerned with security, or any other activities done in the organization to value security.
3. Describe the security awareness, in terms of the effectiveness of security training program, stuffs sense of security, continuous training on information security.
4. Describe the security effectivenesses, in terms of whether the organization has accomplished important security objectives, whether the organisation regularly conducts risk assessment and kept risks to a minimum, whether effective controls are take to protect information security.

Theme Two: Security incident handling and response process.

1. Describe the security incident handling process.
2. Describe the process to learn from the security incident.
3. Describe the effectives in learning from the security incident.
4. Described how the learning of lessons is communicated into the improvements of the security management.
5. Describe the effectiveness of the current methods to communicate the lessons learned from the security incident.

Theme Three: The attitudes towards the GST

1. What are the strengths of the GST?
2. What are weaknesses of the GST?
3. What is your suggestion to improve the weaknesses?
4. What do you suggest to adjust the GST to meet the needs of your organization?
5. Do you have any other comments of the GST?

C.5 Acceptability Questions

1. Using the tool would enhance the effectiveness to communicate lessons learnt from the security incidents.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

2. Using the tool would make it easier to communicate lessons learnt from the security incidents.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

3. I would find the tool useful in communicating lessons learnt from the security incidents.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

4. Learning to use the tool would be easy for me.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

5. My interaction with the tool would be clear and understandable.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

6. I would find the tool easy to use.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

7. Given the resources, opportunities and knowledge it takes to use the tool, it would be easy for me to use the tool.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

8. Using the tool fits into my work style.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

9. Assuming I have access to the tool, I intend to use it.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

10. I am satisfied with the overall experience of the tool.

A. strongly disagree B. disagree C. moderate D. agree E. strongly agree

C.6 Background questionnaire results

Table C.1: Participant's background

No.	Position	Education	Incidents Experience	Gender	Years of Working
1	Nurse	Bachelor	Yes	Female	3
2	Nurse	Bachelor	No	Female	2
3	Nurse	Bachelor	Yes	Female	5
4	Nurse	High School	No	Female	3
5	Nurse	High School	No	Female	4
6	Nurse	High School	No	Female	5
7	Doctor	Master	No	Male	8
8	Doctor	Master	Yes	Male	8
9	Doctor	Bachelor (Hon)	No	Male	4
10	Doctor	Bachelor	No	Male	5
11	IT Manager	Bachelor	Yes	Male	8
12	IT Staff	Master	Yes	Female	4
13	IT Staff	Bachelor (Hon)	Yes	Male	2
14	IT Staff	Bachelor (Hon)	Yes	Male	3
15	IT Staff	Bachelor	Yes	Male	2

Appendix D

The Empirical Experiment (Appendix to Chapter 7)

D.1 Instruction

Instruction: the Creation Steps of the Generic Security Template

Table of Content

Introduction.....2

Step 1: Prepare the *Goal Structure*.....3

Guidance – Prepare the *Top Goal*.....3

Example.....3

Guidance –Prepare the rest of the *Goal Structure*.....3

Example.....3

Step 2: Prepare the *Lessons Learned*.....5

Guidance – Prepare the *Lessons Learned*.....5

Example.....5

Step 3: Map the *Lessons Learned* to the *Goal Structure*.....6

Guidance –Mapping.....6

Step 4: Elaborate *Strategy* and *Context*.....9

Guidance – *Strategy*.....9

Example for *Strategy*.....9

The Generic Security Template with *Strategy* Notation.....10

Guidance – *Context*.....11

Example for *Context*.....11

The Generic Security Template with *Context* Notation.....12

Appendix 1: Password Security Case.....13

Appendix 2: Password Security Guideline.....14

Appendix 3: The Generic Security Template.....15

Introduction

The *Generic Security Template*, is a structured description of lessons learned from the security case. In particular it maps lessons learned to security guidelines using the customised Goal Structuring Notations. The objective is to enhance the sharing of lessons learned from the security incident. This instruction provides the steps on how to create *Generic Security Template* (Appendix 3), from the Case Description (Appendix 1) and a Password Security Guidance in Appendix 2.

Step 1: Prepare the Goal Structure

Guidance – Prepare the Top Goal

- The *Top Goal* is the claim that the whole goal structure is designed to support. It claimed about the security of the system or application.
- It should be stated in the format “<system> is acceptably secure” or “<application> is acceptably secure”.
- The *Case Description* (Appendix 1: Case Description) indicates it is about the password, therefore, create and fill in the *Goal* Notation (depicted as squares) with the statement “Password is acceptably secure”

Example

Input (Appendix 1: Case Description)

As is inferred from the Case Description, the *Top Goal* is “Password is acceptably secure”

Example Output

Password is acceptably Secure

Guidance –Prepare the rest of the Goal Structure

- Again, every *Goal* is a claim made that its sub-goal structure is designed to support.
- Use the structured categories of the security guideline as the *Goal Structure* and place them under the *Top Goal*. In this instruction, we use the *Password Security Guideline* (Appendix 2) as the *Goal Structure*.
- Create and fill in each *Goal* Notation with a single item from the Password Security Guideline (Appendix 2).
- Organise the goals into the *Goal Structure* by converting the text into tree structure.
- Use Arrow (\longrightarrow) to link those *Goals*, it represents supportive relationships.

Example

Input (Appendix 2: Password Security Guideline)

1. Use multiple passwords
- 1.1 Use multiple passwords for different account, systems
-
3. Use long passwords
- 3.1 Keep passwords more than eight characters

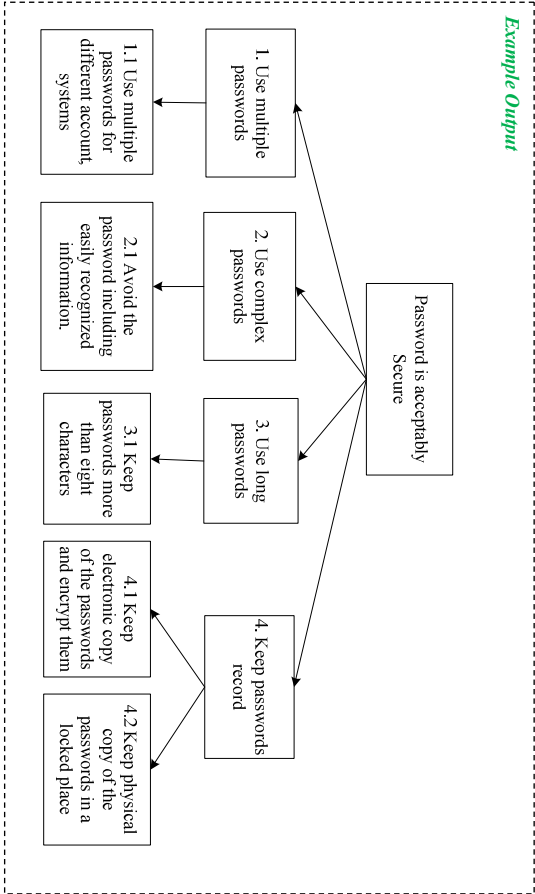


Fig. 1: The Goal Structure

Step 2: Prepare the *Lessons Learned*

Guidance – Prepare the *Lessons Learned*

- The *Lessons Learned* is defined as the knowledge or understanding gained by experience. In this instruction, it refers to,
 - Security Issues (i.e. causes of the security incidents)
 - Security Recommendations (i.e. recommendations intended to prevent the future incident of a similar kind)
- They are provided in the form of structured description, <Security Issue>; <Security Recommendation>
- Fill in each *Lessons Learned* Notation (depicted as circles) with a single item from *Lessons Learned* Section (Appendix 1: Lessons Learned)

Example

Input (Appendix 1: Lessons Learned)

Security Issues	Security Recommendations
Password Sharing	Should not share the password with others
Complex Password	Should use complex password with combination of letters and numbers
Multiple Password:	Should use different password for different account
Password Record	Should keep a password record and ensure the record is securely protected

Example Output

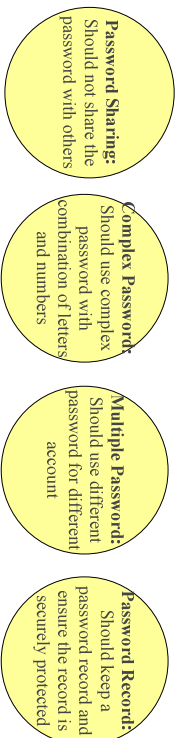


Fig 2: The Lessons Learned Notations

Step 3: Map the *Lessons Learned* to the *Goal Structure*

Guidance –Mapping

Different *Lessons Learned* identified in Step 2 contains different levels of details and can be mapped to different level of the *Goal Structure*. This is a **subjective process that you have to decide the relation between the *Goals* and the *Lessons Learned***. Depending on their relation with the goals, those lessons learned have been divided into four types. Below are the rules to decide the mapping and the types of the *Lessons Learned*.

Decide the Mapping and Lessons Learned Types

Starting from the bottom-level *Goals* in the *Goal Structure*,

- If a *Lessons Learned* is related *exclusively* to a bottom-level *Goal*, it is defined as *Type I*. Then this *Lessons Learned* should be mapped to this bottom-level *Goal*.

Lessons Learned	Related Goal	Type	Mapping
Multiple Password: Should use different password for different account	1.1 Use multiple passwords for different account systems	Type I	Goal 1.1

- If a *Lessons Learned* is related to more than one bottom-level *Goals* in the goal structure, it is defined as *Type II*. Then this *Lessons Learned* should be mapped to the nearest goal where those two bottom-level *Goal* share the same *Parent Goal*.

Lessons Learned	Related Goal	Type	Mapping
Password Record: Should keep a password record and ensure the record is securely protected	4.1 Keep electronic copy of the passwords and encrypt them 4.2 Keep physical copy of this the passwords in a locked place	Type II	(Parent) Goal 4

- If a *Lessons Learned* is related to none of the bottom-level *Goal*, go up to check other *Goals*, check and decide whether it is related to a higher level *Goal* in the structure. If yes, it is defined as *Type III*, this *Lessons Learned* should be mapped to this related *Goal*.

Lessons Learned	Related Goal	Type	Mapping
<div>Complex Password: Should use complex password with combination of letters and numbers</div>	<div>2. Use complex passwords</div>	Type III	Goal 2

- If a *Lessons Learned* is related to none of the *Goals* in the *Goal Structure*, it is defined as *Type IV*, then a new *Goal* named “(Standard non-existent)” should be created to link this *Lessons Learned* to the *Top Goal*.

Lessons Learned	Related Goal	Type	Mapping
	None	Type IV	Create a new goal named “(Standard non-existent)” and link between <i>Top Goal</i> and this <i>Lessons Learned</i>
<div>Password Sharing: Should not share the password with others</div>			(Refer to Fig. 3)

Link Lessons Learned to the Goal Structure

- Link those *Lessons Learned* to the *Goal Structure* according to the Mapping results in the above tables
- Use Arrow (\longrightarrow) to link them, it represents supportive relationships.

Reflect the Lessons Learned Types

- Reflect the *Lessons Learned Types* by filling them in the *Lessons Learned* Notations (refer to Fig. 3)

Clean the Diagrams

- Clean the diagram by deleting the *Goals* that are not mapped to any *Lessons Learned* (refer to Fig. 3) as the final diagram aims to reflect only the mapped *Goals* and *Lessons Learned*.

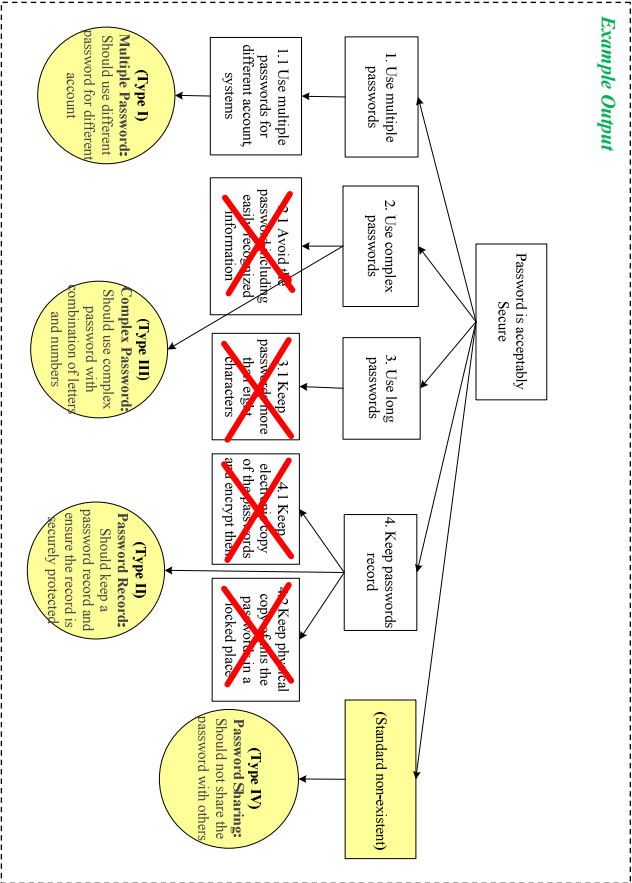


Fig. 3: The Goal Structure with newly mapped Lessons Learned

Step 4: Elaborate Strategy and Context

Guidance – Strategy

- *Strategy* is inserted between *Goals* to provide methods used for the goal decomposition.
 - The statement in the *Strategy* Notation should be in the form “Argument over <approach>”
 - In this instruction, we have used two strategies to decompose the *Goal Structure*.
- Strategy 1*
- We have used *Password Security Guideline* (Appendix 2) as the goal decomposition method.
 - Fill in the *Strategy* Notation (depicted as diamonds) with “Argument over Password Security Guideline”.
 - Insert this *Strategy* Notation into the *Goal Structure* between the *Top Goal* and the *Goal Structure* created from the security guidelines.
 - Use Arrow (—————>) to link them, it represents supportive relationships.
- Strategy 2*
- The goal decomposition method also considers the *Lessons Learned* which are not included in the security guideline.
 - Fill in the *Strategy* Notation with “Argument over All Missing Security Recommendations”.
 - Insert this *Strategy* notation into the *Goal Structure* between the *Top Goal* and the *New Goal* created for Type IV *Lessons Learned*.
 - Use Arrow (—————>) to link them, it represents supportive relationships.

Example for Strategy

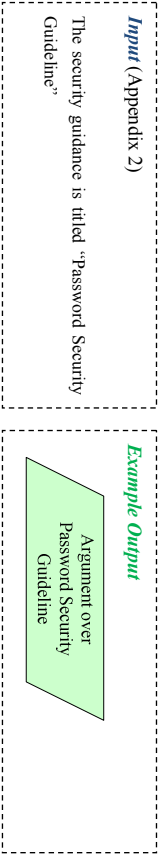


Fig. 4: The Strategy Notation for Strategy 1

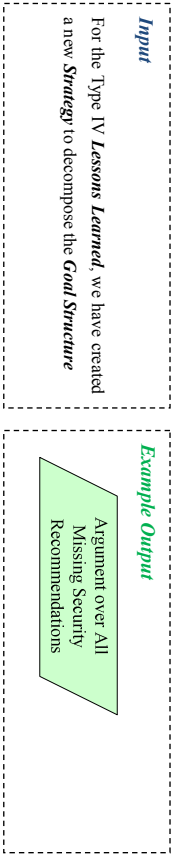


Fig. 5: The Strategy Notation for Strategy 2

The Generic Security Template with Strategy Notation

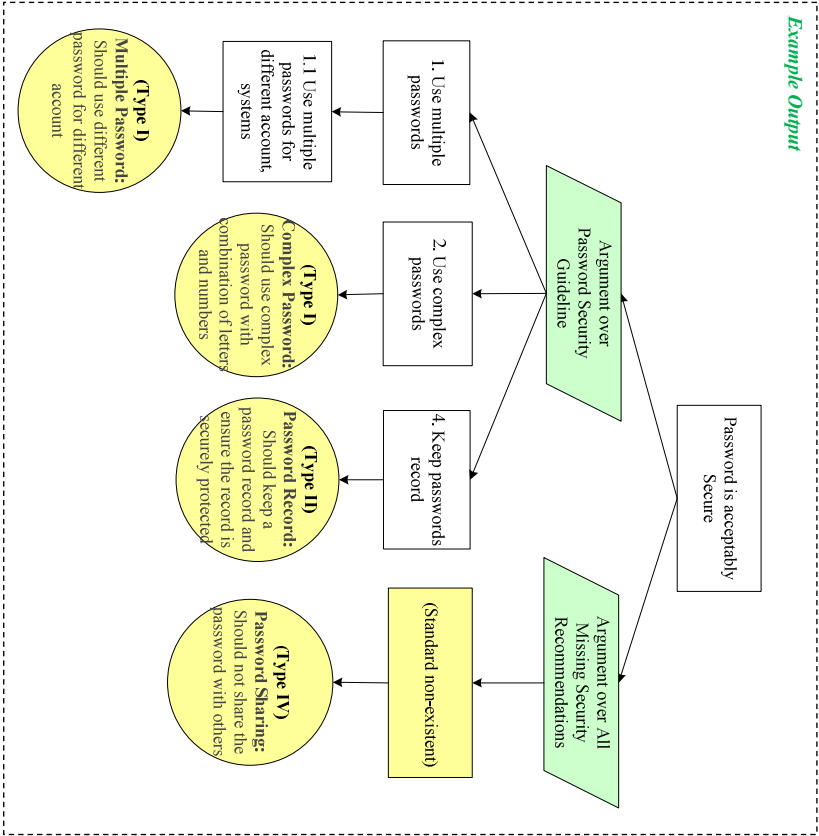


Fig. 6: The Goal Structure with newly added Strategies

Guidance – Context

- Context is used to present supplementary information such as concepts clarification in the claim/strategy.
- The statement in the *Context* notation should be in the form of <Noun-Phrase>
- In this instruction, we have used *Context* notations to elaborate the *Goals* or *Strategies*.

Context

- The Case Description (Appendix 1: Case Description) indicates this incident happened to Alex. Therefore, the *Top Goal* is elaborated with supplementary information “Alex’s Password”.
- Fill in the *Context* Notation with “Alex’s Password”.
- Attach the *Context* Notation into the *Top Goal* “Alex’s Password”.
- Use *Hollow Arrow* (—————>) to link them, it represents the relationship “in context of”.

Fig. 4 has reflected the above changes

Example for Context

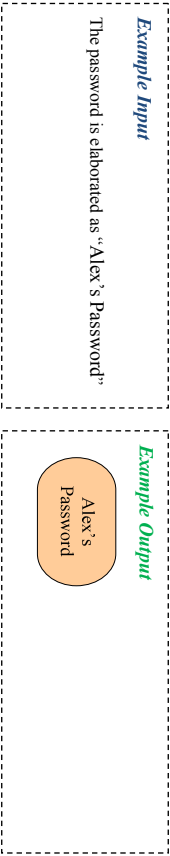


Fig. 7: The Context Notation

The Generic Security Template with Context Notation

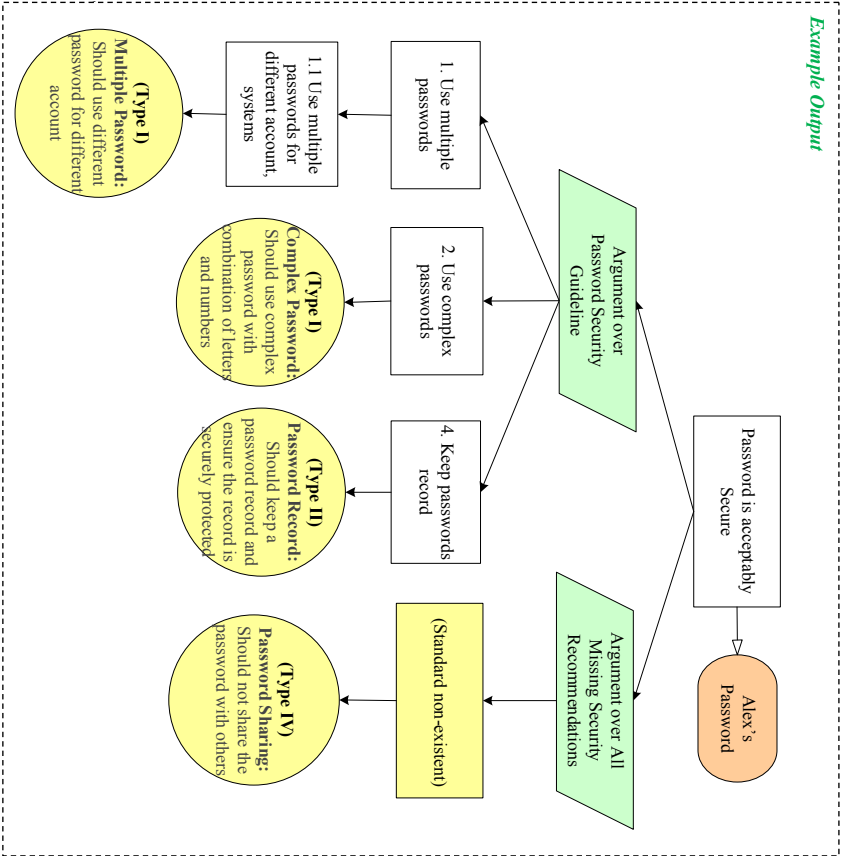


Fig. 8: The Goal Structure with newly added Contexts

Appendix 1: Password Security Case

Case Description

Alex's credit card shows abnormal transactions. He suspects the password was stolen by someone else. An investigation of this case found that his password is the same as Gmail password and has been shared with his friends before. His password has used digit numbers only. The reason he gives for using similar password is, he could not memorize them if using multiple passwords.

Lessons Learned

Security Issues	Security Recommendations
Password Sharing	Should not share the password with others
Complex Password	Should use complex password with combination of letters and numbers
Multiple Password:	Should use different password for different account
Password Record	Should keep a password record and ensure the record is securely protected

Appendix 2: Password Security Guideline

1. Use multiple passwords

1.1 Use multiple passwords for different account, systems
2. Use complex passwords

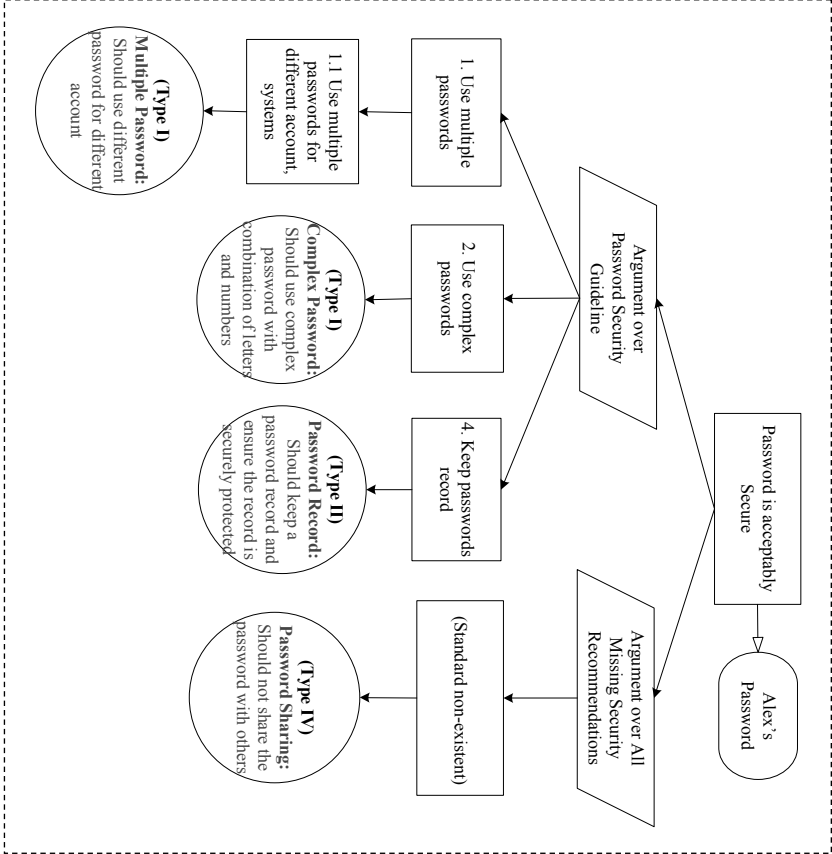
2.1 Avoid the password including easily recognized information.
3. Use long passwords

3.1 Keep passwords more than eight characters
4. Keep passwords record

4.1 Keep electronic copy of the passwords and encrypt them

4.2 Keep physical copy of the passwords in a locked place

Appendix 3: The Generic Security Template



D.2 Participant Consent Form

INTRODUCTION

This research proposes a new incident reporting approach, the Generic Security Template. It is a structured description of the lessons learned from the security incidents. In particular it maps the lessons learned to the security standards or guidelines using the graphical Goal Structuring Notations. The objective is to enhance the sharing of the lessons learnt from the security incident.

STUDY PROCESS

The steps include: (1) study the creation of the Generic Security Template from the instruction; (2) create a Generic Security Template for a tiny case study about the credit card disposing.

BENEFITS

This study aims to familiarize you with this new approach using easy to understand case studies. The benefit you get from this experiment might be (1) a new technique to describe security incidents (2) a few recommendations on how to securely destroy a credit card.

CONFIDENTIALITY

All information collected during this study will be kept strictly confidential; This data might be used as part of research publications and reports in journals, conferences and workshops. However, all reported data will be anonymised and all efforts will be undertaken to prevent participants from being identified.

PARTICIPATION

Your participation in this study is voluntary. If you decide to participate, you may withdraw at any time without penalty.

CONTACT

If you have questions about the study, please contact:

Miss Ying He, Email: yingh@dcs.gla.ac.uk

Prof Chris Johnson, Email: Christopher.Johnson@glasgow.ac.uk

School of Computing Science, University of Glasgow

DECLARATION

“I confirm that I have read and understand the information above. I agree to participate in this study with the understanding that I may withdraw at any time.”

Signed

Date

Contact Information

D.3 Experiment Task - A case on Credit Card Disposing

Task Instruction

- (1) Read the instruction The Creation Steps of the Generic Security Template and learn how to create the Generic Security Template.
- (2) Follow the instruction and create the Generic Security Template, using the Credit Card Disposing Case (Appendix 1) and a Credit Card Disposing Guideline (Appendix 2).
- (3) Write down your answer in the provided answer sheet.
- (4) Fill in a Questionnaire after this exercise.
- (5) Please return your completed Concert Form, Answer Sheet and Questionnaire after this study.

D.3.1 Appendix 1: Credit Card Disposing Case

Case Description

Alex has a credit card which is due to expire; he has cut it off into two pieces and through them away in the trash bin. His friend suggests making additional cuts between at least every four digits on the front of the card. He should also disable the Magnetic Strip. Moreover, he should review the pieces and make sure that no significant amount of information can be retrieved from any one piece. Finally, Instead of throwing them once, he should throw out half of it one week and the second half the following week.

Lessons Learned

Table D.1: Credit Card Disposing

Security Issues	Security Recommendations
Card Destroy	Make additional cuts between at least every four digits on the front of the card
Magnetic Strip	Disable the Magnetic Strip.
Card Destroy	Review the pieces and make sure that no significant amount of information can be retrieved from any one piece.
Card Disposal	Throw out half of the cut pieces one week and the second half the following week.

D.3.2 Appendix 2: Credit Card Disposing Guidelines

1. Disable Magnetic Strip
 - 1.1 Disable the magnetic strip by running a magnet across the strip.
 - 1.2 Take scissors and score the strip to make it unreadable.
2. Destroy Smart Chips/RFIDs
 - 2.1 Smash the Smart Chips/RFIDs with a hammer prior to destroying the card.
3. Destroy the Card
 - 3.1 Burn the cards.
 - 3.2 Cut the card strategically into pieces.
 - 3.2.1 Cut across the numbers and name information of the front of the card
 - 3.2.2 Cut through the signature
4. Dispose of the Card
 - 4.1 Use separate trash cans to dispose of the card.

Figure D.1: Credit Card Disposing Guidelines

D.4 Answer Sheets

Answer Sheet

Step 1: Prepare the *Goal Structure*

Your *Goal Structure* (refer to Fig. 1 on Page 4 of the Instruction as an example answer)

Step 2: Prepare the ***Lessons Learned***

Your ***Lessons Learned*** (refer to Fig. 2 on Page 5 of the Instruction as an example answer)

Step 3: Map the *Lessons Learned* to the *Goal Structure*

Your **Lessons Learned Mapping** (refer to Fig. 3 on Page 8 of the Instruction as an example answer)

* The lessons learned do not necessarily have all four types.

Step 4: Elaborate ***Strategy*** and ***Context***

Your ***Strategy*** (refer to Fig. 4 and Fig. 5 on Page 9 of the Instruction as an example answer)

Your ***Context*** (refer to Fig. 7 on Page 11 of the Instruction as an example answer)

Your Final **Generic Security Template**

Your final **Generic Security Template** (refer to Fig. 8 on Page 12 of the Instruction as an example answer)

Final Check of **Generic Security Template**

Check you **Generic Security Template** if it has satisfied the following criteria

1. Check the main components

It should include the **Goal Structure**, **Lessons Learned**, the **Strategy**, and the **Context**

2. Check you have used the right **Arrows/Hollow Arrows** to present the relationships between different notations

3. Check you have provided the **Types** (e.g. *Type I, II*) **of the Lessons Learned** in the **Lessons Learned** Notation in your final **Generic Security Template**

D.5 Post-Experiment Questionnaire

Section A: Background Information

1. Highest level of degree _____
2. Major subject _____
3. Gender ☐ Male ☐ Female
4. Have you taken information security related courses?
☐ Yes ☐ No
5. Experience with diagramming technique?
☐ Goal Structuring Notations (GSN)
☐ Entity-Relationship (ER)
☐ Unified Modeling Language (UML)
☐ Others, please specify _____

Section B: Obstacles during the creation of the Generic Security Template

6. I have no difficulty in completing the Step 1 while creating the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

If there are difficulties, what are them and your suggestion to improve?

7. I have no difficulty in completing the Step 2 while creating the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

If there are difficulties, what are them and your suggestion to improve?

8. I have no difficulty in completing the Step 3 while creating the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

If there are difficulties, what are them and your suggestion to improve?

9. I have no difficulty in completing the Step 4 while creating the Generic Security Template.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

If there are difficulties, what are them and your suggestion to improve?

10. Any other comments, please specify.

Section C: Task Load Index

Place an “X” along each scale at the point that best indicates your experience.

11. How mentally demanding was the task?

Low ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ High

12. How hurried or rushed was the pace of the task?

Low ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ High

13. How discouraged, stressed, and annoyed did you feel when doing the tasks?

Low ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ High

14. How successful do you feel in accomplishing the task?

Low ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ High

15. How hard did you have to work to complete the task?

Low ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ High

Section D: Usability Evaluation

16. Approximately, how much time you have used for completing this study, including the study of instructions and the creation of the Generic Security Template.

_____ minutes.

17. Learning to use the tool would be easy for me.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

18. I can use it adorably if I am asked to use it again.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

19. I am satisfied with the overall experience of the tool.

A. Strongly disagree B. Disagree C. Neutral D. Agree E. Strongly agree

Appendix E

Industrial Evaluation (Appendix to Chapter 8)

E.1 Acceptance of Recommendations: Shenzhen Data Leakage Incident 2008

Table E.1: Acceptance of Recommendations: Shenzhen Data Leakage Incident 2008

Category	Learning	Current Status and Decisions
Network Security	Protect network security according to the security standard	Current setting uses network physical isolation to ensure the network security. (Implemented with customisation.)
Sensitive Information	Define the information sensitive level	Definition of “sensitive information” is not well understood by the staff, e.g. some staffs define it as medical record only. (Implementable) Action: The organisation should define the information sensitive level.
Security Training	Establish and execute security training programs by following the security standard.	Current training includes only an entrance training program. (Implementable.) Action: A systematic training program is planned to establish by following the security standards.
Security Policy	Establish and enforce security policy according to the security standards	Security policy has been established and enforced by following the Security Standards (GB/T22239). (Implemented.)
Security Audit	Establish and conduct security audit plan according to the security standards	Currently there is no Security Audit Plan. (Implementable.) Action: A security audit plan is planned to establish by following the security standards

E.2 Acceptance of Recommendations: VA Data Leakage Incident 2007

Table E.2: Acceptance of Recommendations: VA Data Leakage Incident 2007

Category	Learning	Current Status and Decisions
Management Structure	Establish an accurate functional description and performance plan to clarify the line authority and reporting relationship.	The organisation felt that their current functional description and performance plan were not accurate and not documented. (Implementable) . Action: Work on a documented functional description and performance plan.
Position description	Re-evaluate and correct position sensitivity levels	“Position sensitivity level” had not been formalized with the organisation. (Implementable with customisation) . Action: Define the position sensitive level.
Risk Analysis	Develop and issue Government-wide risk analysis criteria	Currently, XXX Central Hospital interacts with government wide systems, including the Chinese national insurance system. However, they felt that this recommendation could only be implemented at government level, hence it was not a subject they felt was in their area of responsibility. (Implementation unnecessary) .

Table E.2: (continued)

Category	Learning	Current Status and Decisions
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage.	The Chinese hospital forbids the use of removable media hence this recommendation is not immediately applicable. However, the group could envisage a time when this requirement might be relaxed. If removable media were to be permitted then this recommendation would be an essential requirement for future security. (Reserved for future use).
Security Policy	Ensure that data security plans for research projects comply with information security policies.	Currently, XXX Central Hospital designed data security plans in compliance with information security policies. (Implemented).
Security Policy	Ensure research involving human subjects, compliant with information security requirements;	Currently, XXX Central Hospital conducting research involving human subjects in compliance with "China Personal Information Protection Act". (Implemented with customisation).
Security Policy	Discontinue storing email on unauthorised system.	The Chinese hospital forbids the use of Emails hence this recommendation is not immediately applicable. However, the group could envisage a time when this requirement might be relaxed. If Emails were to be permitted then this recommendation would be an essential requirement for future security. (Reserved for future use).

Table E.2: (continued)

Category	Learning	Current Status and Decisions
Access Control	Avoid the abuse programmer level access granted for research purposes	Currently, there are no issues reported regarding wrongly assigning the access control. (Implementable with customisation) . Action: Implementable through department meeting to warn the security engineers of the consequences caused by wrongly granting access control.
Administrative Action	Take administrative actions against the people involved in this incident for their inappropriate actions according to the “data protection law”	They have taken administrative actions against the people involved in this incident for their inappropriate actions according to the “China Personal Information Protection Act” . (Implemented with customisation) . Action: Take administrative actions against the people involved in this incident for their inappropriate actions according to the “China Personal Information Protection Act”.

E.3 Acceptance of Recommendations: VA Data Leakage Incident 2006

Table E.3: Acceptance of Recommendations: VA Data Leakage Incident 2006

Category	Learning	Current Status and Decisions
Sensitive Information	Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage.	As is mentioned, the Chinese hospital forbids the use of removable media hence this recommendation is not immediately applicable. This recommendation is reserved for future use. (Reserved for future use) .
Position Description	Define the position sensitive level.	“Position sensitivity level” had not been formalized with the organisation. (Implementable) . Action: Define the position sensitive level.
Security Training	Provide linkage to all applicable laws and policy as part of the security awareness training.	The hospital does not provide access to applicable laws and policy as part of the security awareness training. (Implementable) . Action: Provide access to applicable laws and policy.
Incident Handling	Enhance incident-response program on promptly identification and thoroughly investigation of the incidents	Currently, the organisation has not thoroughly investigated the security incidents. (Implementable) . Action: Enhance incident-response program on promptly identification and thoroughly investigation of the incidents.

Table E.3: (continued)

Category	Learning	Current Status and Decisions
Administrative Action	Take administrative actions against the people involved in this incident for their inappropriate actions according to the “data protection law”	They have taken administrative actions against the people involved in this incident for their inappropriate actions according to the “China Personal Information Protection Act” (Implemented with customisation) . Action: Take administrative actions against the people involved in this incident for their inappropriate actions according to the “China Personal Information Protection Act”

Bibliography

- [1] BS7799, “Information security management, BS7799, part 1: code of practice for information security management,” 1999.
- [2] S. Mitropoulos, D. Patsos, and C. Douligieris, “On incident handling and response: A state-of-the-art approach,” *Computers & Security*, vol. 25, no. 5, pp. 351–370, 2006.
- [3] S. Northcutt, *Computer Security Incident Handling: Step by Step, a Survival Guide for Computer Security Incident Handling*. Sans Institute, 2001.
- [4] J. Murray, “Analysis of the incident handling six-step process,” in *SANS Reading Room*, 2007.
- [5] P. Shedden, A. Ahmad, and A. Ruighaver, “Organisational learning and incident response: promoting effective learning through the incident response process,” 2010.
- [6] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident response teams—challenges in supporting the organisational security function,” *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.
- [7] T. P. Kelly, *Arguing safety: a systematic approach to managing safety cases*. University of York, 1999.
- [8] J. R. Landis and G. G. Koch, “The measurement of observer agreement for categorical data,” *biometrics*, pp. 159–174, 1977.
- [9] ENISA, “The ISMS framework,” 2013, <http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework> [Online: accessed 18-Nov-2013].

- [10] R. Bloomfield and P. Bishop, "Safety and assurance cases: Past, present and possible future—an adelard perspective," in *Making Systems Safer*. Springer, 2010, pp. 51–67.
- [11] T. Kelly, "A systematic approach to safety case management," in *Proc. of SAE 2004 World Congress, Detroit, MI*. Citeseer, 2004.
- [12] I. C. Office, "ICO fines NHS Surrey for failing to check the destruction of old computers," 2013, http://www.ico.org.uk/news/latest_news/2013/ico-issues-nhs-surrey-monetary-penalty-of-200000 [Online: accessed 18-Nov-2013].
- [13] C. J. Alberts and A. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.
- [14] U. V. A. Administration, "Review of issues related to the loss of VA information involving the identity of millions of veterans," vol. Report No. 06-02238-163, 2006.
- [15] ———, "Administrative investigation loss of VA information VA medical center birmingham, al," vol. Report No. 07-01083-157, 2007.
- [16] C. E. Healthcare, "Shenzhen hospital data loss incident," 2008, http://www.chinaehc.cn/index.php?option=com_content&view=article&id=1937:2010-04-01-09-38-35&catid=15:medical-reforming&Itemid=15 [Online: accessed 18-Nov-2013].
- [17] Symantec, *Internet Security Threat Report 2013*. Symantec Corporation, 2013, vol. 18.
- [18] ———, *Internet Security Threat Report 2014*. Symantec Corporation, 2014, vol. 19.
- [19] R. T. Mercuri, "The HIPAA-potamus in health care data security," *Communications of the ACM*, vol. 47, no. 7, pp. 25–28, 2004.
- [20] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279–314, 2010.

- [21] T. Porteous, C. Bond, R. Robertson, P. Hannaford, and E. Reiter, "Electronic transfer of prescription-related information: comparing views of patients, general practitioners, and pharmacists." *The British Journal of General Practice*, vol. 53, no. 488, p. 204, 2003.
- [22] C. S. Gadd and L. E. Penrod, "Dichotomy between physicians' and patients' attitudes regarding EMR use during outpatient encounters." in *Proceedings of the AMIA Symposium*. American Medical Informatics Association, 2000, p. 275.
- [23] L. Wardman, "Patients knowledge and expectations of confidentiality in primary health care: a quantitative study," *British Journal of General Practice*, vol. 50, no. 460, pp. 901–902, 2000.
- [24] P. Chhanabhai and A. Holt, "Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures," *Medscape General Medicine*, vol. 9, no. 1, p. 8, 2007.
- [25] G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records," *International journal of medical informatics*, vol. 80, no. 2, pp. 94–101, 2011.
- [26] C. P. Waegemann, "IT security: developing a response to increasing risks," *International journal of bio-medical computing*, vol. 43, no. 1, pp. 5–8, 1996.
- [27] I. C. Office, "Belfast trust fined 225,000 after leaving thousands of patient records in disused hospital," 2012, http://www.ico.org.uk/news/latest_news/2012/belfast-trust-fined-225000-after-leaving-thousands-of-patient-records/-in-disused-hospital-19062012 [Online: accessed 18-Nov-2013].
- [28] —, "NHS trust fined 325,000 following data breach affecting thousands of patients and staff," 2013, http://ico.org.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients/-and-staff-01062012 [Online: accessed 18-Nov-2013].
- [29] —, "Sensitive details of NHS staff published by trust in Devon," 2013, http://ico.org.uk/news/latest_news/2012/

- sensitive-details-of-nhs-staff-published-by-devon-trust-06082012 [Online: accessed 18-Nov-2013].
- [30] N. England, "NHS allocations for 2013/14," 2014, <http://www.england.nhs.uk/allocations-2013-14/> [Online: accessed 19-Sep-2014].
- [31] E. Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," in *European Network and Information Security Agency*, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com.2012.11_en.pdf [Online: accessed 16-05-2012].
- [32] GOV.UK, "Government launches information sharing partnership on cyber security," 2013, <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> [Online: accessed 18-Nov-2013].
- [33] J. H. Eloff and M. Eloff, "Information security management: a new paradigm. SAICSIT; vol. 47," in *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, Pages, pp. 130–136.
- [34] A. Calder, *Information security based on ISO 27001/ISO 17799: a management guide*. Van Haren Publishing, 2006.
- [35] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, and R. Ruefle, "Handbook for computer security incident response teams (csirts)," DTIC Document, Tech. Rep., 2003.
- [36] T. Grance, K. Kent, and B. Kim, "Computer security incident handling guide," *NIST Special Publication*, pp. 800–61, 2004.
- [37] D. L. Cooke, "Learning from incidents," in *21st System Dynamics Conference, NYC, New York*, 2003.
- [38] J. Hadgkiss, "Computer security incident response teams: Exploring the incident learning capability," Ph.D. dissertation, The University of Melbourne Australia, 2006.

- [39] C. Melara, J. M. Sarriegui, J. J. Gonzalez, A. Sawicka, and D. L. Cooke, "A system dynamics model of an insider attack on an information system," in *Proceedings of the 21st International Conference of the System dynamics Society*, 2003, pp. 20–24.
- [40] P. Stephenson, "Conducting incident post mortems," *Computer Fraud & Security*, vol. 2003, no. 4, pp. 16–19, 2003.
- [41] D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology*, vol. 3, no. 1, pp. 61–75, 2004.
- [42] B. S. Institution, "Code of practice for information security management bs ISO/IEC 27002:2005." British Standards Institution, 2008.
- [43] NH-ISAC, "National healthcare and public health resilience," 2013.
- [44] I. C. Office, "NHS Surrey c/o department of health regional legacy management team, Data Protection Act 1998 monetary penalty notice," 2013, http://ico.org.uk/enforcement/~media/documents/library/Data_Protection/Notices/nhs-surrey-monetary-penalty-notice.pdf [Online: accessed 18-Nov-2013].
- [45] Y. He and C. Johnson, "Generic security cases for information system security in healthcare systems," 2012.
- [46] D. H. Robinson and K. A. Kiewra, "Visual argument: Graphic organizers are superior to outlines in improving learning from text." *Journal of Educational Psychology*, vol. 87, no. 3, p. 455, 1995.
- [47] T. P. Kelly, "Concepts and principles of compositional safety case construction," *Contract Research Report for QinetiQ COMSA/2001/1/1*, 2001.
- [48] I. Habli and T. Kelly, "A generic goal-based certification argument for the justification of formal analysis," *Electronic Notes in Theoretical Computer Science*, vol. 238, no. 4, pp. 27–39, 2009.
- [49] Y. He, C. Johnson, K. Renaud, Y. Lu, and S. Jebriel, "An empirical study on the use of the generic security template for structuring the lessons from information security incidents," in *Proceedings of the 6th International Conference on Computer Science and Information Technology*, 2014, pp. 178–188.

- [50] Y. He, C. Johnson, Y. Lu, and Y. Lin, "Improving the information security management: An industrial study in the privacy of electronic patient records," in *The 27th International Symposium on Computer-Based Medical Systems*, 2014.
- [51] Y. He, C. Johnson, Y. Lu, and A. Ahmad, "Improving the exchange of security arguments in security incident reports: Case studies in the privacy of electronic patient records," in *The 8th IFIP WG 11.11 International Conference on Trust Management*, 2014.
- [52] Y. He, C. Johnson, M. Evangelopoulou, and Z.-S. Lin, "Diagraming approach to structure the security lessons: Evaluation using cognitive dimensions," in *The 7th International Conference on Trust & Trustworthy Computing*, 2014.
- [53] K. Scarfone, T. Grance, and K. Masone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, p. 38, 2008.
- [54] P. E. Secchi, "Proceedings of alerts and lessons learned: An effective way to prevent failures and problems (technical report wpp-167)," 1999.
- [55] R. F. Dacey, *Federal Information System Controls Audit Manual (FISCAM)*. DIANE Publishing, 2010.
- [56] C. P. Pfleeger and S. L. Pfleeger, *Security in computing*. Prentice Hall Professional, 2003.
- [57] D. E. R. Denning, *Information warfare and security*. Addison-Wesley Reading MA, 1999, vol. 4.
- [58] D. Gollmann, J. Meier, and A. Sabelfeld, *Computer Security—ESORICS 2006: 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings*. Springer, 2006, vol. 4189.
- [59] G. Dhillon and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Communications of the ACM*, vol. 43, no. 7, pp. 125–128, 2000.
- [60] E. . Youngs', "Fighting to close the gap: Ernst & Young's 2012 global information security survey." Ernst & Youngs', 2012.
- [61] B. S. Institution, "information security management in health using ISO/ IEC 27002 (ISO27799:2008)." British Standards Institution, 2008.

- [62] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002.
- [63] NIST, "National Vulnerability Database," 2013, <http://nvd.nist.gov/> [Online: accessed 18-Nov-2013].
- [64] M. A. Rothstein, "Health privacy in the electronic age," *The Journal of legal medicine*, vol. 28, no. 4, pp. 487–501, 2007.
- [65] T. A. Sykes, V. Venkatesh, and A. Rai, "Explaining physicians' use of EMR systems and performance in the shakedown phase," *Journal of the American Medical Informatics Association*, vol. 18, no. 2, pp. 125–130, 2011.
- [66] T. Greenhalgh, S. Hinder, K. Stramer, T. Bratan, and J. Russell, "Adoption, non-adoption, and abandonment of a personal electronic health record: case study of healthspace," *BMJ: British Medical Journal*, vol. 341, 2010.
- [67] T. C. Rindfleisch, "Privacy, information technology, and health care," *Communications of the ACM*, vol. 40, no. 8, pp. 92–100, 1997.
- [68] C. M. Angst and R. Agarwal, "Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion," *Mis Quarterly*, vol. 33, no. 2, pp. 339–370, 2009.
- [69] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of biomedical informatics*, vol. 46, no. 3, pp. 541–562, 2013.
- [70] M. A. Rothstein and M. K. Talbott, "Compelled authorizations for disclosure of health records: magnitude and implications," *The American Journal of Bioethics*, vol. 7, no. 3, pp. 38–45, 2007.
- [71] L. Zurita and C. Nøhr, "Patient opinion—ehr assessment from the users perspective." *Studies in health technology and informatics*, vol. 107, no. Pt 2, pp. 1333–1336, 2003.
- [72] A. Hoerbst, C. D. Kohl, P. Knaup, and E. Ammenwerth, "Attitudes and behaviors related to the introduction of electronic health records among austrian and german citizens," *International journal of medical informatics*, vol. 79, no. 2, pp. 81–89, 2010.

- [73] M. Wei and X. Xue-guo, "Discussion of patients' confidentiality in sharing electric medical records," *Soft Science of Health*, vol. 3, p. 034, 2009.
- [74] E. Vaast, "Danger is in the eye of the beholders: Social representations of information systems security in healthcare," *The Journal of Strategic Information Systems*, vol. 16, no. 2, pp. 130–152, 2007.
- [75] G. N. Samy, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems," *Health informatics journal*, vol. 16, no. 3, pp. 201–209, 2010.
- [76] K. T. Win, "A review of security of electronic health records," *Health Information Management*, vol. 34, no. 1, pp. 13–18, 2005.
- [77] J. Hu, H.-H. Chen, and T.-W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Computer Standards & Interfaces*, vol. 32, no. 5, pp. 274–280, 2010.
- [78] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing," *Computer Communications*, vol. 31, no. 4, pp. 760–769, 2008.
- [79] B. Blobel, "Authorisation and access control for electronic health record systems," *International journal of medical informatics*, vol. 73, no. 3, pp. 251–257, 2004.
- [80] G. H. Motta and S. S. Furuie, "A contextual role-based access control authorization model for electronic patient record," *Information Technology in Biomedicine*, vol. 7, no. 3, pp. 202–207, 2003.
- [81] K. D. Mandl, W. W. Simons, W. C. Crawford, and J. M. Abbett, "Indivo: a personally controlled health record for health information exchange and communication," *BMC medical informatics and decision making*, vol. 7, no. 1, p. 25, 2007.
- [82] D. Gritzalis and C. Lambrinoudakis, "A security architecture for interconnecting health information systems," *International Journal of Medical Informatics*, vol. 73, no. 3, pp. 305–309, 2004.

- [83] M. Farzandipour, F. Sadoughi, M. Ahmadi, and I. Karimi, "Security requirements and solutions in electronic health records: lessons learned from a comparative study," *Journal of medical systems*, vol. 34, no. 4, pp. 629–642, 2010.
- [84] S. Pahnla, M. Siponen, and A. Mahmood, "Employees' behavior towards is security policy compliance," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, 2007, pp. 156b–156b.
- [85] M. Dekker and S. Etalle, "Audit-based access control for electronic health records," *Electronic Notes in Theoretical Computer Science*, vol. 168, pp. 221–236, 2007.
- [86] L. Rostad and O. Edsberg, "A study of access control requirements for health-care systems based on audit trails from access logs," in *Computer Security Applications Conference*. IEEE, 2006, pp. 175–186.
- [87] S. Kahn and V. Sheshadri, "Medical record privacy and security in a digital environment," *IT professional*, vol. 10, no. 2, pp. 46–52, 2008.
- [88] B. S. Elger, J. Iavindrasana, L. Lo Iacono, H. Müller, N. Roduit, P. Summers, and J. Wright, "Strategies for health data exchange for secondary, cross-institutional clinical research," *Computer methods and programs in biomedicine*, vol. 99, no. 3, pp. 230–251, 2010.
- [89] P. D. Clayton, W. Boebert, G. Defriese, S. Dowell, M. Fennell, K. Frawley, J. Glaser, R. Kemmerer, C. Landwehr, T. Rindfleisch *et al.*, "For the record: protecting electronic health information," *National Research Council.(Washington, DC: National Academy Press, 1997)*, 1997.
- [90] E. ISO, "27799: 2008 health informatics," *Information security management in health using ISO/IEC*, vol. 27002, 2008.
- [91] J. S. Broderick, "ISMS, security standards and security regulations," *information security technical report*, vol. 11, no. 1, pp. 26–31, 2006.
- [92] W. E. Deming, "Out of the crisis," *Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study*, p. 6, 1986.
- [93] W. Boehmer, "Analysis of strongly and weakly coupled management systems in information security," in *The Fourth International Conference on Emerging*

- Security Information Systems and Technologies (SECURWARE)*. IEEE, 2010, pp. 109–116.
- [94] R. B. Ness *et al.*, “Influence of the hipaa privacy rule on health research,” *JAMA: the journal of the American Medical Association*, vol. 298, no. 18, pp. 2164–2170, 2007.
- [95] F. C. C. W. Team, “Data Protection Act,” 2008.
- [96] —, “Tele-communication and internet personal information protection act,” <http://www.miit.gov.cn/n11293472/n11294912/n11296542/15514014.html> [Online: accessed 18-Nov-2013].
- [97] C. P. Team, “Cmmi for development, version 1.2,” 2006.
- [98] “GB/T22239-2008 information security technology - base line for classified protection of information system,” 2008.
- [99] F. Cervone, “ITIL: a framework for managing digital library services,” *OCLC Systems & Services*, vol. 24, no. 2, pp. 87–90, 2008.
- [100] D. Mellado, E. Fernández-Medina, and M. Piattini, “A common criteria based security requirements engineering process for the development of secure information systems,” *Computer standards & interfaces*, vol. 29, no. 2, pp. 244–253, 2007.
- [101] T. Lodderstedt, D. Basin, and J. Doser, “SecureUML: A UML-based modeling language for model-driven security,” in *UML 2002 The Unified Modeling Language*. Springer, 2002, pp. 426–441.
- [102] G. Ridley, J. Young, and P. Carroll, “COBIT and its utilization: A framework from the literature,” in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. IEEE, 2004, pp. 8–pp.
- [103] U. S. P. Law, *Federal Information Security Management Act (FISMA)*. 116 STAT. 2899, 2002.
- [104] S. NIST, “800-53,” *Recommended Security Controls for Federal Information Systems*, pp. 800–53, 2007.

- [105] P. Bowen, J. Hash, and M. Wilson, “SP 800-100. SP 800-100. information security handbook: A guide for managers,” 2006.
- [106] M. of Health of People’s republic of China, “Guidance on the classified protection of information system by ministry of health,” 2011, http://www.gov.cn/gzdt/2011-12/09/content_2016113.htm [Online: accessed 18-Nov-2013].
- [107] B. Von Solms, “Information security - the third wave?” *Computers & Security*, vol. 19, no. 7, pp. 615–620, 2000.
- [108] R. Von Solms, “Information security management: why standards are important,” *Information Management & Computer Security*, vol. 7, no. 1, pp. 50–58, 1999.
- [109] K. Höne and J. H. P. Eloff, “Information security policywhat do international information security standards say?” *Computers & Security*, vol. 21, no. 5, pp. 402–409, 2002.
- [110] R. Gomes and L. V. Lapão, “The adoption of IT security standards in a health-care environment,” *Studies in health technology and informatics*, vol. 136, p. 765, 2008.
- [111] T. Wiander, “Implementing the ISO/ IEC 17799 standard in practice-findings from small and medium sized software organisations,” in *5th International Conference on Standardization and Innovation in Information Technology*. IEEE, 2007, pp. 91–104.
- [112] M. Siponen, “Information security standards focus on the existence of process, not its content,” *Communications of the ACM*, vol. 49, no. 8, pp. 97–100, 2006.
- [113] M. Siponen and R. Willison, “Information security management standards: Problems and solutions,” *Information & Management*, vol. 46, no. 5, pp. 267–270, 2009.
- [114] D. S. Herrmann, *Using the Common Criteria for IT security evaluation*. CRC Press, 2002.
- [115] D. Basin, J. Doser, and T. Lodderstedt, “Model driven security: From uml models to access control infrastructures,” *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 15, no. 1, pp. 39–91, 2006.

- [116] H. F. Tipton and M. Krause, *Information security management handbook*. CRC Press, 2003.
- [117] W. Muhren, G. Van Den Eede, and B. Van de Walle, “Organisational learning for the incident management process: Lessons from high reliability organisations,” in *Journal of Information Systems Security*, 2008.
- [118] P. Stephenson, “Conducting incident post mortems,” in *Computer Fraud and Security*, 2003.
- [119] H. Cavusoglu, B. Mishra, and S. Raghunathan, “A model for evaluating it security investments,” *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004.
- [120] K. J. S. Hoo, *How much is enough? A risk management approach to computer security*. Stanford University, 2000.
- [121] W. Sonnenreich, J. Albanese, and B. Stout, “Return on security investment (rosi)-a practical quantitative model,” *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 45–56, 2006.
- [122] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.
- [123] A. A. Tan T, Ruighaver AB, “Incident handling: where the need for planning is often not recognised,” in *Preceedings of the 1st Australian Computer Network, Information & Forensics Conference*, 2003.
- [124] Y.-C. Chang, *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing, 2012.
- [125] M. R. K. Nicole FALESSI, Razvan GAVRILA and K. MOULINOS, “National cyber security strategies,” 2012.
- [126] cisp.org.uk, “CISP - Cyber-Security Information Sharing Partnership,” 2014, <https://www.cisp.org.uk/> [Online: accessed 18-Aug-2014].
- [127] M. Dekker and C. Karsberg, “Annual incident reports 2011,” 2012.

- [128] D. C. Dimitra Liveri and L. Dupr, “Technical guideline on reporting incidents article13a implementation,” 2011.
- [129] M. Daneman and P. A. Carpenter, “Individual differences in working memory and reading,” *Journal of verbal learning and verbal behavior*, vol. 19, no. 4, pp. 450–466, 1980.
- [130] J. H. Larkin and H. A. Simon, “Why a diagram is (sometimes) worth ten thousand words,” *Cognitive science*, vol. 11, no. 1, pp. 65–100, 1987.
- [131] J. M. Paige and H. A. Simon, “Cognitive processes in solving algebra word problems,” *Problem solving: Research, method, and theory*, pp. 15–16, 1966.
- [132] H. C. Purchase, “Twelve years of diagrams research,” *Journal of Visual Languages & Computing*, 2013.
- [133] S. Price, “Processing animation: Integrating information from animated diagrams,” in *Diagrammatic Representation and Inference*. Springer, 2004, pp. 360–364.
- [134] N. Swoboda and G. Allwein, “Modeling heterogeneous systems,” in *Diagrammatic Representation and Inference*. Springer, 2002, pp. 131–145.
- [135] R. McCartney and P. El-Kafrawy, “Inter-diagrammatic reasoning and digital geometry,” in *Diagrammatic Representation and Inference*. Springer, 2004, pp. 199–215.
- [136] L. R. Novick and K. M. Catley, “Interpreting hierarchical structure: Evidence from cladograms in biology,” in *Diagrammatic Representation and Inference*. Springer, 2006, pp. 176–180.
- [137] F. Ruskey and M. Weston, “A survey of venn diagrams,” *Electronic Journal of Combinatorics*, vol. 4, 1997.
- [138] J. Rumbaugh, I. Jacobson, and G. Booch, *Unified Modeling Language Reference Manual, The*. Pearson Higher Education, 2004.
- [139] C. Johnson, “Proving properties of accidents,” *Reliability Engineering & System Safety*, vol. 67, no. 2, pp. 175–191, 2000.

- [140] P. Chinneck, D. Pumfrey, and T. Kelly, "Turning up the heat on safety case construction," in *Practical Elements of Safety*. Springer, 2004, pp. 223–240.
- [141] A. Greenough and H. Graham, "Protecting and using patient information: the role of the caldicott guardian," *Clinical medicine*, vol. 4, no. 3, pp. 246–249, 2004.
- [142] N. Direct, "National framework for reporting and learning from serious incidents requiring investigation," 2010, <http://www.nrls.npsa.nhs.uk/resources/?entryid45=75173> [Online: accessed 18-Nov-2013].
- [143] L. Mei and Y. Ling, "A study on issues and strategies concerning the IT-based security system for whole people health," *China Science & Technology Resources Review*, vol. 4, p. 009, 2010.
- [144] C.-D. Wang, W.-B. Yang, and S.-G. Ju, "Research and implementation of electronic health record signature system based on ces," *Computer Engineering*, vol. 16, p. 103, 2010.
- [145] J. Xian-shan, "Security control of computer-based patient record," *Information of Medical Equipment*, vol. 2, p. 008, 2006.
- [146] P. SHEN, X.-y. HU, S.-g. ZHANG, and D.-j. DU, "Informationalized characteristics of medical records management and risk prevention," *Journal of Medical Postgraduates*, vol. 10, p. 021, 2009.
- [147] Y. Cangzhou, L. Zhongkan, and Z. Qishan, "A security scheme for electronic medical record systems," *Computer Engineering*, vol. 9, p. 050, 2004.
- [148] X. Gao, J. Xu, G. Sorwar, and P. Croll, "Implementation of e-health record systems and e-medical record systems in china," *The International Technology Management Review*, vol. 3, no. 2, pp. 127–139, 2013.
- [149] B. S. Alhaqbani, "Privacy and trust management for electronic health records," 2010.
- [150] O. U. Press, "Oxford dictionary online," 2013, <http://www.oxforddictionaries.com/definition/english/argument?q=argument> [Online: accessed 18-Nov-2013].

- [151] T. Govier, *A Practical Study of Argument Enhanced Edition*. Cengage Learning, 2013.
- [152] J. Górski, “Trust casea case for trustworthiness of IT infrastructures,” in *Cyberspace Security and Defense: Research Issues*. Springer, 2005, pp. 125–141.
- [153] R. Bloomfield, P. Bishop, C. Jones, and P. Froome, “ASCAD - Adelard Safety Case Development Manual,” 1998.
- [154] U. M. of Defence, “00-56 safety management requirements for defence systems.” Ministry of Defence, 2007.
- [155] G. Despotou, T. Kelly, S. White, and M. Ryan, “Introducing safety cases for health IT,” in *4th International Workshop on Software Engineering in Health Care (SEHC)*. IEEE, 2012, pp. 44–50.
- [156] I. . 2:2011, “ISO/ IEC 15026 - 2:2011, systems and software assurance,” 2011.
- [157] C. B. Weinstock, H. F. Lipson, and J. Goodenough, “Arguing security-creating security assurance cases.”
- [158] J. L. Vivas, I. Agudo, and J. López, “A methodology for security assurance-driven system development,” *Requirements Engineering*, vol. 16, no. 1, pp. 55–73, 2011.
- [159] C. Alexander, S. Ishikawa, and M. Silverstein, “Pattern languages,” *Center for Environmental Structure*, vol. 2, 1977.
- [160] S. Lautieri, D. Cooper, and D. Jackson, “Safsec: Commonalities between safety and security assurance,” in *Constituents of Modern System-safety Thinking*. Springer, 2005, pp. 65–75.
- [161] P. Graydon, I. Habli, R. Hawkins, T. Kelly, and J. Knight, “Arguing conformance,” *Software, IEEE*, vol. 29, no. 3, pp. 50–57, 2012.
- [162] P. J. Graydon and T. P. Kelly, “Using argumentation to evaluate software assurance standards,” *Information and Software Technology*, vol. 55, no. 9, pp. 1551–1562, 2013.
- [163] G. F. Cooper, “The computational complexity of probabilistic inference using bayesian belief networks,” *Artificial intelligence*, vol. 42, no. 2, pp. 393–405, 1990.

- [164] C. M. Holloway, "Safety case notations: alternatives for the non-graphically inclined?" in *3rd IET International Conference on System Safety*. IET, 2008, pp. 1–6.
- [165] O. U. Press, "Oxford dictionary online," 2013, <http://www.oxforddictionaries.com/definition/english/generic/> [Online: accessed 18-Nov-2013].
- [166] W. S. Greenwell, "A taxonomy of fallacies in system safety arguments william s. greenwell; university of virginia; charlottesville, virginia, usa john c. knight; university of virginia, charlottesville, virginia, usa c. michael holloway; nasa langley research center; hampton, virginia, usa jacob j. pease; university of virginia; charlottesville, virginia, usa," *Red Herring*, vol. 1, p. 1, 2006.
- [167] R. Lawton and D. Parker, "Barriers to incident reporting in a healthcare system," *Quality and Safety in Health Care*, vol. 11, no. 1, pp. 15–18, 2002.
- [168] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design patterns: Abstraction and reuse of object-oriented design*. Springer, 1993.
- [169] T. Kelly and S. B. Meng, "The costs, benefits, and risks associated with pattern-based and modular safety case development," in *in Proceedings of the UK MoD Equipment Safety Assurance Symposium*. Citeseer, 2005.
- [170] I. C. Office, "IT asset disposal for organisations - Data Protection Act," 2012, http://ico.org.uk/news/latest_news/2013/~media/documents/library/Data_Protection/Detailed_specialist_guides/it_asset_disposal_for_organisations_20121.pdf [Online: accessed 18-Nov-2013].
- [171] C. W. Johnson, "Lessons from major incidents influencing and influenced by telecoms failures," *Crisis Management: Concepts, Methodologies, Tools and Applications*, p. 311, 2014.
- [172] F. S. Authority, "Data security in financial services," 2008, http://www.fsa.gov.uk/pubs/other/data_security.pdf [Online: accessed 20-Aug-2014].
- [173] B. News, "Zurich insurance fined 2.3m over customers' data loss," 2010, <http://www.bbc.co.uk/news/business-11070217> [Online: accessed 20-Aug-2014].
- [174] I. C. Office, "ICO fines glasgow city council 150k," 2013, http://www.ico.org.uk/news/latest_news/2013/ico-issues-nhs-surrey-monetary-penalty-of-200000 [Online: accessed 20-Aug-2014].

- [175] H.-F. Hsieh and S. E. Shannon, “Three approaches to qualitative content analysis,” *Qualitative health research*, vol. 15, no. 9, pp. 1277–1288, 2005.
- [176] D. Craigen, “Formal methods technology transfer: Impediments and innovation,” in *CONCUR’95: Concurrency Theory*. Springer, 1995, pp. 328–332.
- [177] M. G. Hinchey, “Confessions of a formal methodist,” in *SCS*, 2002, pp. 17–20.
- [178] K. Finney and A. Fedorec, “An empirical study of specification readability,” *Teaching and Learning Formal Methods*, Academic Press, New York, 1996.
- [179] D. Carew, C. Exton, and J. Buckley, “An empirical investigation of the comprehensibility of requirements specifications,” in *2005 International Symposium on Empirical Software Engineering*. IEEE, 2005, pp. 10–pp.
- [180] R. Razali, C. Snook, M. Poppleton, P. Garratt, and R. Walters, “Usability assessment of a UML-based formal modelling method,” in *19th Annual Psychology of Programming Workshop (PPIG’07)*, 2007, pp. 56–71.
- [181] M. I. Bauer and P. N. Johnson-Laird, “How diagrams can improve reasoning,” *Psychological Science*, vol. 4, no. 6, pp. 372–378, 1993.
- [182] K. Stenning and J. Oberlander, “A cognitive theory of graphical and linguistic reasoning: Logic and implementation,” *Cognitive science*, vol. 19, no. 1, pp. 97–140, 1995.
- [183] M. Petre, “Why looking isn’t always seeing: readership skills and graphical programming,” *Communications of the ACM*, vol. 38, no. 6, pp. 33–44, 1995.
- [184] E. Folmer and J. Bosch, “Architecting for usability: a survey,” *Journal of systems and software*, vol. 70, no. 1, pp. 61–78, 2004.
- [185] S. G. Hart and L. E. Staveland, “Development of NASA-TLX (task load index): Results of empirical and theoretical research,” *Human mental workload*, vol. 1, no. 3, pp. 139–183, 1988.
- [186] R. Dewar, “Design and evaluation of graphic symbols,” *Proceedings of public graphics*, vol. 24, pp. 1–25, 1994.
- [187] J. A. Stoner, “Cross-over trials in clinical research,” *Journal of the American Statistical Association*, vol. 99, no. 468, pp. 1208–1208, 2004.

- [188] B. S. Everitt, *The analysis of contingency tables*. CRC Press, 1992, vol. 45.
- [189] T. R. Green, "Cognitive dimensions of notations," 1989, pp. 443–460.
- [190] M. Kutar, C. Britton, and T. Barker, "A comparison of empirical study and cognitive dimensions analysis in the evaluation of UML diagrams," in *Procs of the 14th Workshop of the Psychology of Programming Interest Group (PPIG 14)*, 2002.
- [191] E. Triffitt and B. Khazaei, *A study of usability of Z formalism based on cognitive dimensions*, 2002.
- [192] A. F. Blackwell and T. R. Green, "A cognitive dimensions questionnaire optimised for users," in *Proceedings of the Twelfth Annual Meeting of the Psychology of Programming Interest Group*, 2000, pp. 137–152.
- [193] D. T. Campbell, J. C. Stanley, and N. L. Gage, *Experimental and quasi-experimental designs for research*. Houghton Mifflin Boston, 1963.
- [194] P. Shoval and S. Shiran, "Entity-relationship and object-oriented data modeling-an experimental comparison of design quality," vol. 21, no. 3. Elsevier, 1997, pp. 297–315.
- [195] C. Glezer, M. Last, E. Nachmany, and P. Shoval, "Quality and comprehension of UML interaction diagrams-an experimental comparison," vol. 47, no. 10. Elsevier, 2005, pp. 675–692.
- [196] R. K. Yin, *Case study research: Design and methods*. sage, 2003, vol. 5.
- [197] Y. Fan, "A classification of chinese culture," *Cross Cultural Management: An International Journal*, vol. 7, no. 2, pp. 3–10, 2000.
- [198] W. Qiufang *et al.*, "Foreign language testing - a study on the implementation of the national oral test for english majors-band 8," *Foreign Language World*, vol. 5, 2005.
- [199] P. Y. Logan and D. Noles, "Protecting patient information in outsourced tele-health services: Bolting on security when it cannot be baked in," *International Journal of Information Security and Privacy (IJISP)*, vol. 2, no. 3, pp. 55–70, 2008.

- [200] Q. Ma, A. C. Johnston, and J. M. Pearson, "Information security management objectives and practices: a parsimonious framework," *Information Management & Computer Security*, vol. 16, no. 3, pp. 251–270, 2008.
- [201] D. Lending and T. W. Dillon, "The effects of confidentiality on nursing self-efficacy with information systems," *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 2, no. 3, pp. 49–64, 2007.
- [202] B. D. Medlin and J. A. Cazier, "An empirical investigation: health care employee passwords and their crack times in relationship to hipaa security standards," *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 2, no. 3, pp. 39–48, 2007.
- [203] J. D'Arcy and A. Hovav, "Does one size fit all? examining the differential effects of IS security countermeasures," *Journal of business ethics*, vol. 89, no. 1, pp. 59–71, 2009.
- [204] M. Fishbein and I. Ajzen, *Belief, attitude, intention and behavior: An introduction to theory and research*, 1975.
- [205] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly*, pp. 319–340, 1989.
- [206] R. J. Vallerand and C. F. Ratelle, "Intrinsic and extrinsic motivation: A hierarchical model," *Handbook of self-determination research*, vol. 128, pp. 37–63, 2002.
- [207] I. Ajzen, "The theory of planned behavior," *Organizational behavior and human decision processes*, vol. 50, no. 2, pp. 179–211, 1991.
- [208] S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," *Information systems research*, vol. 6, no. 2, pp. 144–176, 1995.
- [209] R. L. Thompson, C. A. Higgins, and J. M. Howell, "Influence of experience on personal computer utilization: testing a conceptual model," *Journal of management information systems*, vol. 11, no. 1, pp. 167–187, 1994.
- [210] E. M. Rogers and F. F. Shoemaker, "Communication of innovations: A cross-cultural approach," 1971.

- [211] A. Bandura, *Social foundations of thought and action*. Englewood Cliffs, NJ Prentice Hall., 1986.
- [212] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view." *MIS quarterly*, vol. 27, no. 3, 2003.
- [213] B. J. Oates, *Researching information systems and computing*. Sage, 2005.
- [214] A. D. Veiga and J. H. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007.
- [215] S. K. Katsikas, "Health care management and information systems security: awareness, training or education?" *International journal of medical informatics*, vol. 60, no. 2, pp. 129–135, 2000.
- [216] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *computers & security*, vol. 25, no. 4, pp. 289–296, 2006.
- [217] O. Winkel, "Electronic government and network security: a viewpoint," *Transforming Government: People, Process and Policy*, vol. 1, no. 3, pp. 220–229, 2007.
- [218] W. J. Orlikowski and D. C. Gash, "Technological frames: making sense of information technology in organizations," *ACM Transactions on Information Systems (TOIS)*, vol. 12, no. 2, pp. 174–207, 1994.
- [219] D. R. Denison and A. K. Mishra, "Toward a theory of organizational culture and effectiveness," *Organization science*, vol. 6, no. 2, pp. 204–223, 1995.
- [220] S. E. Chang and C.-S. Lin, "Exploring organizational culture for information security management," *Industrial Management & Data Systems*, vol. 107, no. 3, pp. 438–458, 2007.
- [221] J. Leach, "Improving user security behaviour," *Computers & Security*, vol. 22, no. 8, pp. 685–692, 2003.
- [222] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, 2005.

- [223] D. W. Straub Jr, "Effective IS security: An empirical study," *Information Systems Research*, vol. 1, no. 3, pp. 255–276, 1990.
- [224] E. Madriz, "Focus groups in feminist research," *Collecting and interpreting qualitative materials*, vol. 2, pp. 363–388, 2003.
- [225] D. L. Morgan, *Focus groups as qualitative research*. Sage Publications, Inc, 1988.
- [226] G. Greenleaf, "China's proposed personal information protection act," 2008.
- [227] M. Flood and I. Habli, "Multi-view safety cases," 2011.
- [228] T. R. Peltier, *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press, 2013.
- [229] G. Grispos, W. B. Glisson, and T. Storer, "Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization," *arXiv preprint arXiv:1306.2477*, 2013.
- [230] R. Breu, U. Hinkel, C. Hofmann, C. Klein, B. Paech, B. Rumpe, and V. Thurner, *Towards a formalization of the unified modeling language*. Springer, 1997.
- [231] W. E. McUmber and B. H. Cheng, "A general framework for formalizing uml with formal languages," in *Proceedings of the 23rd international conference on Software engineering*. IEEE Computer Society, 2001, pp. 433–442.
- [232] P. Schobbens, P. Heymans, and J.-C. Trigaux, "Feature diagrams: A survey and a formal semantics," in *14th IEEE international conference on Requirements Engineering*. IEEE, 2006, pp. 139–148.
- [233] A. Evans, R. France, K. Lano, and B. Rumpe, "The UML as a formal modeling notation," in *The Unified Modeling Language. UML'98: Beyond the Notation*. Springer, 1999, pp. 336–348.
- [234] A. Polyvyanyy, S. Smirnov, and M. Weske, "Process model abstraction: A slider approach," in *12th International IEEE Enterprise Distributed Object Computing Conference*. IEEE, 2008, pp. 325–331.
- [235] S. Smirnov, "Structural aspects of business process diagram abstraction," in *IEEE Conference on Commerce and Enterprise Computing*. IEEE, 2009, pp. 375–382.

- [236] T. J. Bench-Capon and P. E. Dunne, “Argumentation in artificial intelligence,” *Artificial intelligence*, vol. 171, no. 10, pp. 619–641, 2007.
- [237] J. Mackinlay, “Automating the design of graphical presentations of relational information,” *ACM Transactions on Graphics (TOG)*, vol. 5, no. 2, pp. 110–141, 1986.
- [238] M. Negnevitsky, *Artificial intelligence: a guide to intelligent systems*. Pearson Education, 2005.
- [239] A. LLP, “ASCE 4.1 SR2,” 2013, <http://www.adelard.com/asce/choosing-asce/gsn.html> [Online: accessed 18-April-2014].
- [240] I. E. S. System, “INESS GSN Tool Manual,” 2012, http://www.iness.eu/IMG/pdf/GSN-Tool_Manual_2012-01-20.pdf [Online: accessed 18-April-2014].
- [241] R. Hawkins, T. Kelly, J. Knight, and P. Graydon, “A new approach to creating clear safety arguments,” in *Advances in Systems Safety*. Springer, 2011, pp. 3–23.
- [242] J. Rushby, “Formalism in safety cases,” in *Making Systems Safer*. Springer, 2010, pp. 3–17.
- [243] E. Denney, G. Pai, and I. Habli, “Towards measurement of confidence in safety cases,” in *2011 International Symposium on Empirical Software Engineering and Measurement (ESEM)*. IEEE, 2011, pp. 380–383.